International Journal of Electronic Devices and Networking

E-ISSN: 2708-4485
P-ISSN: 2708-4477
IJEDN 2024; 5(1): 01-07

www.electronicnetjournal.com
Received: 03-11-2023
Accepted: 11-12-2023

Rishabh
AIT-CSE, Chandigarh University, Mohali, Punjab, India

Saksham Azad
AIT-CSE, Chandigarh University, Mohali, Punjab, India

Corresponding Author:
Rishabh
AIT-CSE, Chandigarh University, Mohali, Punjab, India

Multilayered voice authentication systems

Rishabh and Saksham Azad

DOI: https://doi.org/10.22271/27084477.2024.v5.i1a.46

Abstract
Voice authentication systems play a pivotal role in verifying individuals' identities and ensuring secure access to confidential information. In this research, we introduce a novel approach to enhance the security and robustness of voice authentication by implementing dynamic pitch modulation and tone variations. Our Voice Authentication System employs a multi-layered security architecture to counteract impersonation attempts, including AI voice-based attacks. The research begins with a comprehensive literature review that explores the existing voice authentication systems, identifies their limitations, and proposes an innovative solution. The project's objective is to create a voice authentication system that not only matches voice components for standard authentication but also dynamically alters pitch, frequency, and tone for enhanced security. We detail the methodologies used for data collection, feature extraction, and the implementation of voice component matching, dynamic pitch modulation, and frequency and tone variations. The system's architecture incorporates standard authentication, high-pitch authentication, and low-pitch authentication layers, each with specific security protocols and encryption mechanisms. The implementation phase encompasses software development, hardware integration, and rigorous testing, ensuring the system's reliability and accuracy. User interaction and interface design prioritize a seamless and user-friendly experience while maintaining high security standards. Ethical considerations are paramount, addressing user data privacy and implementing anti-impersonation measures. The results and evaluation section discusses performance metrics, resistance to impersonation attacks, and user feedback, confirming the system's effectiveness and usability. In conclusion, this research contributes to the advancement of voice authentication systems by providing a multi-layered approach that safeguards against emerging threats, including AI-based impersonation. It also outlines future research directions to further enhance voice authentication technology.

Keywords: Component, formatting, style, styling, insert

1. Introduction

1.1 Problem Definition

In today's increasingly digital world, secure authentication mechanisms are of paramount importance. Voice authentication systems have emerged as a robust method to verify the identity of individuals, preventing unauthorized access to sensitive data and services. However, with the advancements in artificial intelligence and machine learning, the risk of voice impersonation, or voice-based attacks, has become a significant concern. Ensuring the reliability and security of voice authentication is a pressing challenge that demands innovative solutions. [1]

1.2 Project Overview

This research project presents a comprehensive exploration of a novel approach to voice authentication, which integrates dynamic pitch modulation and tone variations into the authentication process. Our Voice Authentication System (VAS) is designed to enhance the security of voice authentication by implementing a multi-layered approach, combining standard voice matching with dynamic pitch alterations and frequency modulation. These layers are intended to create an additional level of security, rendering voice impersonation attacks, particularly those driven by AI-generated voices, more challenging. [2]

1.3 Hardware Specification

To achieve the goals of this project, specific hardware components have been carefully selected to facilitate voice data collection, processing, and analysis.

The hardware infrastructure is designed to support the necessary software applications and algorithms for voice authentication. [3]

1.4 Software Specification

The software aspect of the VAS encompasses the development of voice recognition algorithms, dynamic pitch modulation techniques, and frequency and tone variation mechanisms. These software components are instrumental in implementing the multi-layered approach, as well as ensuring user-friendly interfaces and robust security features. [4]

In the following sections, we will delve deeper into the existing voice authentication systems, identifying their limitations and challenges. We will present the proposed system and its innovative approach, outlining the methodology used in data collection, feature extraction, and the implementation of dynamic pitch modulation. Furthermore, we will discuss the system's architecture, software development, hardware integration, and user interaction design. [5]

2. Literature Review

Voice authentication systems have gained prominence as a reliable method for identity verification and secure access to digital services. [8] In this section, we provide an extensive review of existing voice authentication systems, highlight the challenges faced by these systems, introduce our proposed system, and offer a summary of the literature review.

2.1 Existing Voice Authentication Systems

Voice authentication has witnessed significant evolution in recent years, with various systems and technologies coming to the forefront. These systems primarily rely on the analysis of acoustic features and voiceprints to verify the identity of users. Some notable existing systems include These systems have proven effective but are not without their limitations. [9]

While existing systems offer a high degree of accuracy in standard authentication, they are vulnerable to evolving threats, particularly voice-based attacks driven by artificial intelligence. This vulnerability is a result of their limited capability to adapt to new challenges and technologies. [10]

2.2 Challenges in Voice Authentication

Challenges in the field of voice authentication stem from a variety of factors, including:

Impersonation Attacks: Malicious actors can mimic voices with remarkable accuracy, leading to impersonation attacks. The rise of AI-generated voices exacerbates this issue.

Data Privacy: Concerns surrounding the collection, storage, and use of voice data have raised ethical questions regarding user privacy. [11]

Usability: Balancing security and user convenience remains a challenge. Authentication processes must be both secure and user-friendly. [12]

Emerging Threats: As technology advances, so do the capabilities of potential attackers. It is crucial for voice authentication systems to adapt to new threats. [13]

2.3 Proposed System and Enhancements

In response to the identified challenges and vulnerabilities in existing voice authentication systems, our research proposes an innovative Voice Authentication System (VAS) that enhances security through dynamic pitch modulation and tone variations. This multi-layered approach aims to deter impersonation attempts, even those originating from AI-generated voices. [6]

The VAS integrates standard voice matching with dynamic pitch modulation, frequency and tone variation, and robust security protocols. This approach is designed to make impersonation significantly more challenging, thus increasing the overall security of voice authentication systems. [7]

2.4 Literature Review Summary

In summary, the literature review has provided an in-depth examination of existing voice authentication systems, the challenges they face, and the proposed enhancements in our VAS. The vulnerabilities of current systems necessitate the development of more secure and adaptable methods. The subsequent sections will delve into the details of our VAS, including its methodology, experimental setup, results, and future work, highlighting its potential to advance the field of voice authentication.

3. Problem Formulation

The field of voice authentication, while promising in its ability to provide secure identity verification, faces several critical challenges and problems that need to be addressed. This section formulates the key problems that underpin the rationale for the development of our Voice Authentication System (VAS). [15]

3.1 Vulnerability to Impersonation Attacks

One of the primary challenges faced by existing voice authentication systems is their vulnerability to impersonation attacks. Malicious actors can exploit the limitations of current systems to mimic voices, potentially gaining unauthorized access to sensitive information or services. This vulnerability has been exacerbated by the emergence of AI-generated voices, which are becoming increasingly convincing. [14]

3.2 Ethical and Privacy Concerns

The collection and storage of user voice data for authentication purposes raise significant ethical and privacy concerns. Users are rightfully concerned about the security and privacy of their voice biometric data, highlighting the need for systems that prioritize data protection and user consent. [16]

3.3 The Need for Multi-Layered Security

To address these challenges, there is a pressing need for voice authentication systems that incorporate multi-layered security measures. [17] Single-factor authentication systems are no longer sufficient to withstand evolving threats. Thus, the problem formulation extends to the development of a more comprehensive approach that enhances security while maintaining usability.

3.4 Adaptation to Emerging Threats

The rapidly evolving landscape of technology and the increasing sophistication of potential attackers necessitate

voice authentication systems that can adapt to emerging threats. [18] The problem formulation extends to the development of systems capable of detecting and countering new attack methods effectively.

3.5 Balancing Security and Usability
An ongoing challenge in voice authentication is the delicate balance between security and usability. While enhancing security is crucial, it must not come at the expense of user convenience. [19] Striking this balance is a problem that requires innovative solutions.

In this context, our research project aims to address these problem areas by introducing a Voice Authentication System that integrates dynamic pitch modulation, frequency and tone variations, and robust security protocols. [20] By doing so, we aim to enhance security, deter impersonation attacks, and ensure data privacy, offering a comprehensive solution to the identified problems in the field of voice authentication. [21]

4. Research Objectives
To address the challenges and problem areas identified in the field of voice authentication, our research project sets forth the following research objectives:

4.1 Develop a Multi-Layered Voice Authentication System
The primary objective of this research is to develop a Voice Authentication System (VAS) that incorporates multi-layered security measures. This system will go beyond standard voice matching and incorporate dynamic pitch modulation, frequency and tone variations, and robust security protocols to enhance security and deter impersonation attacks.

4.2 Enhance Resistance to Impersonation Attacks
Our research aims to enhance the resistance of the VAS to impersonation attacks, particularly those driven by AI-generated voices. By introducing dynamic pitch modulation and tone variations, the system should become significantly more challenging to mimic or impersonate, increasing the overall security of voice authentication.

4.3 Ensure Data Privacy and Ethical Considerations
We intend to address the ethical and privacy concerns surrounding voice biometric data by implementing strict data privacy measures and obtaining user consent. The research objective is to ensure that our VAS is in compliance with ethical standards and regulatory requirements.

4.4 Maintain Usability and User-Friendliness
While enhancing security is a core objective, we also aim to maintain a high level of usability and user-friendliness. The VAS should provide a seamless and convenient user experience, striking a balance between security and user convenience.

4.5 Evaluate System Performance
Another key objective is to rigorously evaluate the performance of the VAS. This involves conducting comprehensive testing, analyzing system accuracy, and assessing its resistance to impersonation attacks. User feedback and usability testing will also contribute to the evaluation.

4.6 Identify Future Research Directions
In addition to the immediate objectives, this research aims to identify future research directions in the field of voice authentication. [22] It will consider emerging threats, evolving technologies, and user expectations, providing insights into how voice authentication can continue to evolve to meet the security challenges of tomorrow.

5. Methodologies
This section outlines the methodologies used in the development and implementation of the Voice Authentication System (VAS) with a focus on enhancing security and deterring impersonation attacks.

5.1 Data Collection and Preparation
To create a robust voice authentication system, we commence with the collection of diverse voice samples. This phase involves gathering a dataset of voice recordings from a wide range of users. The collected data is then meticulously prepared, including noise reduction, voice activity detection, and standardization of sample formats. [23]

5.2 Feature Extraction and Analysis
Feature extraction plays a pivotal role in voice authentication. Our research utilizes state-of-the-art feature extraction techniques to identify distinctive vocal characteristics. These features may include spectral analysis, pitch, formants, and various other acoustic properties essential for voice recognition.

5.3 Voice Component Matching
In the standard authentication layer of the VAS, voice component matching is performed. This stage employs the extracted features to compare the user's voice with a stored voiceprint. [24] A matching score is calculated to determine the authenticity of the user.

5.4 Dynamic Pitch Modulation
To enhance security and deter impersonation, dynamic pitch modulation is introduced. This method involves altering the pitch of the user's voice in real-time during the authentication process. [25] By doing so, we add an additional layer of complexity, making it challenging for malicious actors to imitate the user's voice accurately.

5.5 Frequency and Tone Variations
Frequency and tone variations are also incorporated into the VAS. In this layer, we introduce dynamic variations in both frequency and tone to further disrupt impersonation attempts. [26] By modulating these aspects of the user's voice, we create a robust defense against voice-based attacks.

5.6 Integration of Security Layers
The methodologies described above are integrated to create a multi-layered security system. The combination of standard voice matching, dynamic pitch modulation, and frequency and tone variations results in a comprehensive approach to voice authentication. This integration ensures that the VAS is resilient against evolving threats and impersonation attacks.

6. System Architecture

The architecture of the Voice Authentication System (VAS) is designed to incorporate multiple authentication layers, each serving a unique purpose in enhancing security and deterring impersonation attacks. [27] The following sections detail the components of the system architecture.

6.1 Standard Authentication Layer

The standard authentication layer is the foundation of the VAS. It utilizes traditional voice matching techniques, including voiceprint comparison and feature analysis, to verify the identity of the user. [28] This layer serves as the primary means of authentication, ensuring a reliable baseline for user recognition.

6.2 High-Pitch Authentication Layer

The high-pitch authentication layer introduces dynamic pitch modulation to the authentication process. During this stage, the user's voice pitch is modulated to a higher frequency. [29] This modulation adds an extra security dimension, making it significantly more challenging for malicious actors to mimic the user's voice accurately. High-pitch authentication acts as a robust countermeasure against voice-based impersonation.

6.3 Low-Pitch Authentication Layer

In contrast to the high-pitch layer, the low-pitch authentication layer applies dynamic pitch modulation to lower the user's voice pitch. This additional security measure further complicates impersonation attempts. The low-pitch layer complements the high-pitch layer, making it increasingly difficult for attackers to imitate the user's voice.

6.4 Security Protocols and Encryption

To safeguard user voice data and the authentication process, the VAS incorporates rigorous security protocols and encryption mechanisms. User voice data is encrypted during transmission and storage, and access control measures are implemented to protect sensitive biometric information. Additionally, the system adheres to established data protection regulations and ethical guidelines to ensure user privacy and security. [30]

The architecture of the VAS is designed to provide a comprehensive and adaptable solution to the challenges of voice authentication. By integrating these distinct authentication layers and security protocols, the system offers a robust defense against impersonation attacks and evolving threats. The balance between traditional voice matching and dynamic pitch modulation enhances both security and user-friendliness, ensuring that the VAS is a valuable addition to the field of voice authentication.

7. Implementation

The implementation phase of the Voice Authentication System (VAS) involves the development of the software, integration with hardware components, comprehensive testing, and the establishment of the user authentication workflow. This section provides an overview of the implementation process.

7.1 Software Development

The software development phase is a critical aspect of the VAS implementation. This includes the creation of the user interface, backend algorithms for voice authentication, and the integration of dynamic pitch modulation, frequency and tone variations, and security protocols. Specialized software tools and programming languages are utilized to build a secure and user-friendly VAS.

7.2 Hardware Integration

In parallel with software development, hardware integration takes place. This phase involves the setup and configuration of the necessary hardware components, including microphones, audio processing units, and server infrastructure. The seamless interaction between software and hardware is crucial for the reliable operation of the VAS.

7.3 Testing and Quality Assurance

Testing and quality assurance are fundamental to ensuring the reliability and security of the VAS. Rigorous testing procedures are applied to evaluate the system's performance, including accuracy in voice authentication, resistance to impersonation attacks, and overall system stability. Quality assurance measures are taken to identify and rectify any software or hardware issues.

7.4 User Authentication Workflow

The user authentication workflow is a pivotal element in the implementation process. This involves creating a user-friendly interface for enrolling and verifying users, capturing voice samples, and guiding users through the authentication process. The workflow is designed to strike a balance between security and convenience, ensuring a smooth user experience.

The implementation phase is critical in bringing the VAS from a conceptual idea to a functional and secure system. The coordination of software and hardware elements, rigorous testing, and the design of the user authentication workflow are all integral to the successful deployment of the VAS. The collaborative efforts of software developers, hardware engineers, and quality assurance specialists contribute to the achievement of the system's objectives.

8. User Interaction

The user interaction aspect of the Voice Authentication System (VAS) is fundamental in ensuring a positive user experience while maintaining robust security measures. This section explores the design of the user interface and the overall user experience.

8.1 Interface Design

8.1.1 User-Friendly Enrollment and Authentication

The design of the VAS interface is oriented toward user-friendliness. During the enrollment process, users are guided through the steps required to capture their voice samples. The interface provides clear instructions and feedback to help users complete the enrollment efficiently. Authentication prompts are designed to be intuitive and straightforward, ensuring a seamless user experience.

8.1.2 Multi-Layered Authentication Interface

The interface also incorporates elements related to the multi-layered authentication approach. Users are informed about the dynamic pitch modulation, frequency and tone variations, and their role in enhancing security. Visual indicators may be provided to inform users about the specific authentication layers employed during each session.

8.2 User Experience

8.2.1 Security-Usability Balance

A key focus in the VAS design is to strike a balance between security and usability. While the system incorporates advanced security measures, the user experience remains a priority. The user experience is optimized to ensure that the VAS is accessible and user-friendly without compromising on security.

8.2.2 Feedback and Guidance

Users receive real-time feedback during authentication attempts. Clear guidance is provided to ensure users understand the process and are aware of the security layers in place. Feedback may include prompts for pitch modulation and frequency variations, aiding users in the successful completion of the authentication process.

8.2.3 Error Handling and Support

A robust error-handling mechanism is integrated to address situations where authentication may fail. Users are guided on how to resolve authentication issues and are provided with appropriate support resources. This ensures that the VAS is reliable even in cases of user errors.

The design of the user interaction in the VAS is a crucial aspect of the system's success. By prioritizing user-friendliness and providing clear guidance, the VAS aims to deliver a secure and accessible voice authentication solution that meets the needs of both security-conscious organizations and end users.

9. Ethical Considerations

The development and deployment of the Voice Authentication System (VAS) necessitate a careful evaluation of ethical considerations to safeguard user data privacy and enhance security while mitigating impersonation risks. [31]

9.1 User Data Privacy

9.1.1 Informed Consent

User data privacy is of paramount importance in the VAS. Prior to enrolling in the system, users are required to provide informed consent. They are made aware of the data collection, storage, and usage practices, including the storage of voice samples for authentication purposes.

9.1.2 Data Encryption and Protection

Voice data collected by the VAS is encrypted during transmission and storage. Security protocols are in place to safeguard sensitive biometric information. The system adheres to data protection regulations and guidelines to ensure the privacy of user data. [32]

9.1.3 User Control and Data Deletion

Users have the option to control their data. They can request the deletion of their voice samples from the system at any time. Additionally, they are provided with mechanisms to review and update their consent settings. [33]

9.2 Security and Anti-Impersonation Measures

9.2.1 Mitigating Impersonation Risks

A core ethical consideration is the protection against impersonation and identity theft. The VAS implements multi-layered security measures, including dynamic pitch modulation, frequency and tone variations, and security protocols to mitigate impersonation risks. These measures are designed to safeguard users' identities and maintain system integrity.

9.2.2 Ethical Use of Biometric Data

The use of biometric voice data is governed by ethical principles. The VAS ensures that the data is utilized solely for authentication purposes and is not shared or repurposed for other objectives. Users can trust that their biometric data is handled with the utmost care and only used in accordance with their consent.

9.2.3 Transparent Security Practices

The VAS maintains transparency in its security practices. Users are informed about the security layers employed during authentication and how these layers contribute to their protection. Transparency fosters trust and helps users understand the security measures in place.

Ethical considerations are integral to the development and operation of the VAS. By prioritizing user data privacy, implementing stringent security measures, and maintaining transparency, the system seeks to strike a balance between technological advancements and ethical responsibility.

10. Results and Evaluation

The effectiveness of the Voice Authentication System (VAS) is assessed through comprehensive evaluation processes that encompass various dimensions of performance, security, and user experience.

10.1 Performance Metrics

10.1.1 Authentication Accuracy

Authentication accuracy is a fundamental performance metric. It measures the system's ability to correctly authenticate legitimate users. The VAS is evaluated on its ability to recognize enrolled users accurately.

10.1.2 False Acceptance Rate (FAR) and False Rejection Rate (FRR)

The FAR and FRR are critical metrics in evaluating the VAS's performance. They assess the system's propensity to falsely accept unauthorized users (FAR) or reject legitimate users (FRR). Achieving a balance between these rates is crucial.

10.2 Resistance to Impersonation Attacks

10.2.1 Dynamic Pitch Modulation

The VAS's resistance to impersonation attacks, especially in the presence of dynamic pitch modulation, is assessed. This measure gauges the system's capability to differentiate between genuine users and impersonators attempting to mimic enrolled voices. [34]

10.2.2 Frequency and Tone Variations

The effectiveness of the frequency and tone variation layers is evaluated. These measures are integral in countering impersonation attempts. The system's ability to detect and respond to variations is a key performance aspect.

10.3 Usability and User Feedback

10.3.1 User Satisfaction

User satisfaction is evaluated through feedback and surveys. Users are asked to provide insights into their experience with the VAS, including ease of use and overall satisfaction.

10.3.2 Error Rates and User Support
The incidence of errors during authentication attempts is recorded, and the effectiveness of user support in addressing these errors is assessed. This measure reflects the system's usability and user-friendliness.

The results and evaluation section provides a comprehensive overview of the VAS's performance and its ability to resist impersonation attacks. The system's accuracy, security, and user-friendliness are key aspects in assessing its suitability for practical applications.

11. Conclusion
The Voice Authentication System (VAS) represents a significant advancement in the field of biometric authentication, offering a multi-layered security approach while prioritizing user data privacy and user experience. This section summarizes the contributions of the VAS, discusses its implications for voice authentication, and outlines future research directions.

11.1 Summary of Contributions
The VAS introduces several noteworthy contributions:

11.1.1 Multi-Layered Authentication
The VAS leverages multi-layered authentication, including dynamic pitch modulation, frequency and tone variations, and security protocols. These layers enhance the security of voice-based authentication and resist impersonation attacks effectively.

11.1.2 User Data Privacy
User data privacy is a central tenet of the VAS. The system implements robust encryption and data protection measures, ensuring that user voice samples are handled with care and in accordance with data protection regulations.

11.1.3 User-Friendly Interface
The user interface of the VAS is designed to prioritize user-friendliness. Clear guidance, informed consent, and user control over their data contribute to a positive user experience.

11.2 Implications for Voice Authentication
The VAS carries important implications for the broader field of voice authentication:

11.2.1 Enhanced Security Measures
The multi-layered approach to authentication, including pitch modulation and frequency variations, offers enhanced security in voice authentication. This can pave the way for more secure voice-based authentication systems in various domains, from financial services to access control.

11.2.2 Ethical Considerations in Biometrics
The VAS's emphasis on data privacy and ethical data handling sets a precedent for responsible biometric data management. Ethical considerations are becoming increasingly important in biometric applications, and the VAS exemplifies best practices.

11.3 Future Work and Research Directions
11.3.1 Continuous Improvement
Future work on the VAS will involve continuous improvement and refinement of the system. This includes optimizing performance metrics, enhancing usability, and refining security measures.

11.3.2 Expanding Applications
The VAS has the potential to be deployed in various sectors beyond its current applications. Future research may explore its use in healthcare, e-commerce, and secure communication systems.

11.3.3 Voice-Based AI and IoT Integration
Exploring the integration of voice-based authentication with artificial intelligence (AI) and Internet of Things (IoT) systems is a promising research direction. This can lead to more sophisticated and secure voice authentication solutions.

In conclusion, the Voice Authentication System (VAS) represents a significant advancement in the domain of voice authentication. Its multi-layered approach, ethical considerations, and implications for enhanced security and user experience hold promise for its adoption in various industries. The VAS's journey continues with a commitment to continuous improvement and the exploration of new research frontiers.

12. References

1. Khan AMHK, *et al*. Voice Biometrics for User Authentication and Authentication Systems - A Literature Review. International Journal of Applied Engineering and Management Letters (IJAEML). 2023;6(1):203-210.
2. Srinivas Publication. Voice Biometric Systems for User Identification and Authentication; c2022.
3. International Journal of Applied Engineering and Management Letters (IJAEML). Android-based Voice Biometric Identity Authentication System; c2022.
4. Sharma S, Tyagi A, Kumar S, Kaushik P. Additive manufacturing process based EOQ model under the effect of pandemic COVID-19 on non-instantaneous deteriorating items with price dependent demand. In A. Editor & B. Editor (Eds.), Additive Manufacturing in Industry 4.0 (1st ed.). CRC Press; c2022.
5. Balamurugan A, Krishna MV, Bhattacharya R, Mohammed S, Haralayya B, Kaushik P. Robotic Process Automation (RPA) in Accounting and Auditing of Business and Financial Information. The British Journal of Administrative Management. 2022;58(157):127-142.
6. IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET). Voice Recognition System for User Authentication Using Gaussian Mixture Model; c2022.
7. SSRN - Search eLibrary. Enhancing Internet Service Security with Voice Biometric Authentication; c2022.
8. IEEE 4th International Conference on Computer and Communications (ICCC). Authentication Model for IoT Devices Using Voice Biometrics; c2022.
9. ResearchGate. Voice Biometrics: An Authentication Method Using Your Voice; c2023.
10. Springer Nature. On the User Experience of Voice-Based Authentication Systems; c2021.
11. ACM Transactions on Computer-Human Interaction (TOCHI). Voice Authentication Systems: A User Experience Perspective; c2020.
12. ACM SIGCHI Conference on Human Factors in

Computing Systems. Designing Voice Authentication Systems for a Better User Experience; c2019.
13. Chopra Y, Kaushik P, Rathore SPS, Kaur P. Uncovering Semantic Inconsistencies and Deceptive Language in False News Using Deep Learning and NLP Techniques for Effective Management. International Journal on Recent and Innovation Trends in Computing and Communication. 2023;11(8s):681-692. https://doi.org/10.17762/ijritcc.v11i8s.7256
14. Kaushik P. Role and Application of Artificial Intelligence in Business Analytics: A Critical Evaluation. International Journal for Global Academic & Scientific Research. 2022;1(3):01-11. https://doi.org/10.55938/ijgasr.v1i3.15
15. Kaushik P. Deep Learning Unveils Hidden Insights: Advancing Brain Tumor Diagnosis. International Journal for Global Academic & Scientific Research. 2023;2(2):01-22. https://doi.org/10.55938/ijgasr.v2i2.45
16. Kaushik P. Unleashing the Power of Multi-Agent Deep Learning: Cyber-Attack Detection in IoT. International Journal for Global Academic & Scientific Research. 2023;2(2):23-45. https://doi.org/10.55938/ijgasr.v2i2.46
17. Kaushik P, Rathore SPS. Deep Learning Multi-Agent Model for Phishing Cyber-attack Detection. International Journal on Recent and Innovation Trends in Computing and Communication. 2023;11(9s):680-686. https://doi.org/10.17762/ijritcc.v11i9s.7674
18. Kaushik P, Miglani S, Shandilya I, Singh A, Saini D, Singh A. HR Functions Productivity Boost by using AI. International Journal on Recent and Innovation Trends in Computing and Communication. 2023;11(8s):701-713. https://doi.org/10.17762/ijritcc.v11i8s.7672
19. Kaushik P, Singh Rathore SPS, Kaur P, Kumar H, Tyagi N. Leveraging Multiscale Adaptive Object Detection and Contrastive Feature Learning for Customer Behavior Analysis in Retail Settings. International Journal on Recent and Innovation Trends in Computing and Communication. 2023;11(6s):326-343. https://doi.org/10.17762/ijritcc.v11i6s.6938
20. Kaushik P, Yadav R. Reliability design protocol and block chain locating technique for mobile agent Journal of Advances in Science and Technology (JAST). 2017;14(1):136-141. https://doi.org/10.29070/JAST
21. Kaushik P, Yadav R. Deployment of Location Management Protocol and Fault Tolerant Technique for Mobile Agents. Journal of Advances and Scholarly Researches in Allied Education (JASRAE). 2018;15(6):590-595. https://doi.org/10.29070/JASRAE
22. Kaushik P, Yadav R. Mobile Image Vision and Image Processing Reliability Design for Fault-Free Tolerance in Traffic Jam. Journal of Advances and Scholarly Researches in Allied Education (JASRAE). 2018;15(6):606-611. https://doi.org/10.29070/JASRAE
23. Kaushik P, Yadav R. Reliability Design Protocol and Blockchain Locating Technique for Mobile Agents Journal of Advances and Scholarly Researches in Allied Education (JASRAE). 2018;15(6):590-595. https://doi.org/10.29070/JASRAE
24. Kaushik P, Yadav R. Traffic Congestion Articulation Control Using Mobile Cloud Computing Journal of Advances and Scholarly Researches in Allied Education (JASRAE). 2018;15(1):1439-1442. https://doi.org/10.29070/JASRAE
25. Pratap Singh Rathore S. Analysing the efficacy of training strategies in enhancing productivity and advancement in profession: theoretical analysis in Indian context. International Journal for Global Academic & Scientific Research. 2023;2(2):56-77. https://doi.org/10.55938/ijgasr.v2i2.49
26. Pratap Singh Rathore S. The Impact of AI on Recruitment and Selection Processes: Analysing the role of AI in automating and enhancing recruitment and selection procedures. International Journal for Global Academic & Scientific Research. 2023;2(2):78-93. https://doi.org/10.55938/ijgasr.v2i2.50
27. Rachna Rathore. Application of Assignment Problem and Traffic Intensity in Minimization of Traffic Congestion. IJRST. 2021;11(3):25-34. DOI: http://doi.org/10.37648/ijrst.v11i03.003
28. Rathore R. A Review on Study of application of queueing models in Hospital sector. International Journal for Global Academic & Scientific Research. 2022;1(2):01-05. https://doi.org/10.55938/ijgasr.v1i2.11
29. Rathore R. A Study on Application of Stochastic Queuing Models for Control of Congestion and Crowding. International Journal for Global Academic & Scientific Research. 2022;1(1):01-07. https://doi.org/10.55938/ijgasr.v1i1.6
30. Rathore R. A Study of Bed Occupancy Management in the Healthcare System Using The M/M/C Queue And Probability. International Journal for Global Academic & Scientific Research. 2023;2(1):01-09. https://doi.org/10.55938/ijgasr.v2i1.36
31. Dua S, Islam M. [Title not available]. Available from: https://web.archive.org/web/20210624021145id_/https://irojournals.com/aicn/V3/I2/03.pdf
32. Sharma T, Kaushik P. Leveraging Sentiment Analysis for Twitter Data to Uncover User Opinions and Emotions. International Journal on Recent and Innovation Trends in Computing and Communication. 2023;11(8s):162-169. https://doi.org/10.17762/ijritcc.v11i8s.7186
33. Sharma V. A Study on Data Scaling Methods for Machine Learning. International Journal for Global Academic & Scientific Research. 2022;1(1):23-33. https://doi.org/10.55938/ijgasr.v1i1.4
34. Yadav M, Kakkar M, Kaushik P. Harnessing Artificial Intelligence to Empower HR Processes and Drive Enhanced Efficiency in the Workplace to Boost Productivity. International Journal on Recent and Innovation Trends in Computing and Communication. 2023;11(8s):381-390. https://doi.org/10.17762/ijritcc.v11i8s.7218