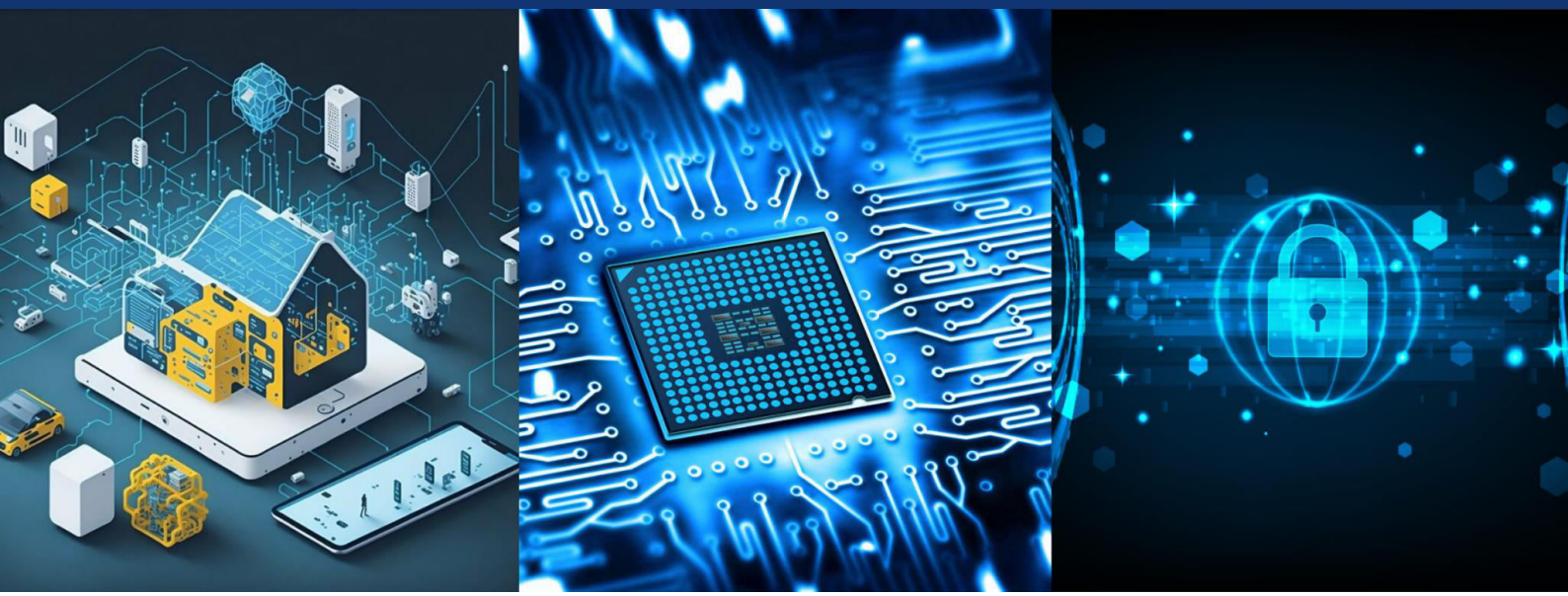
IJIRCCE

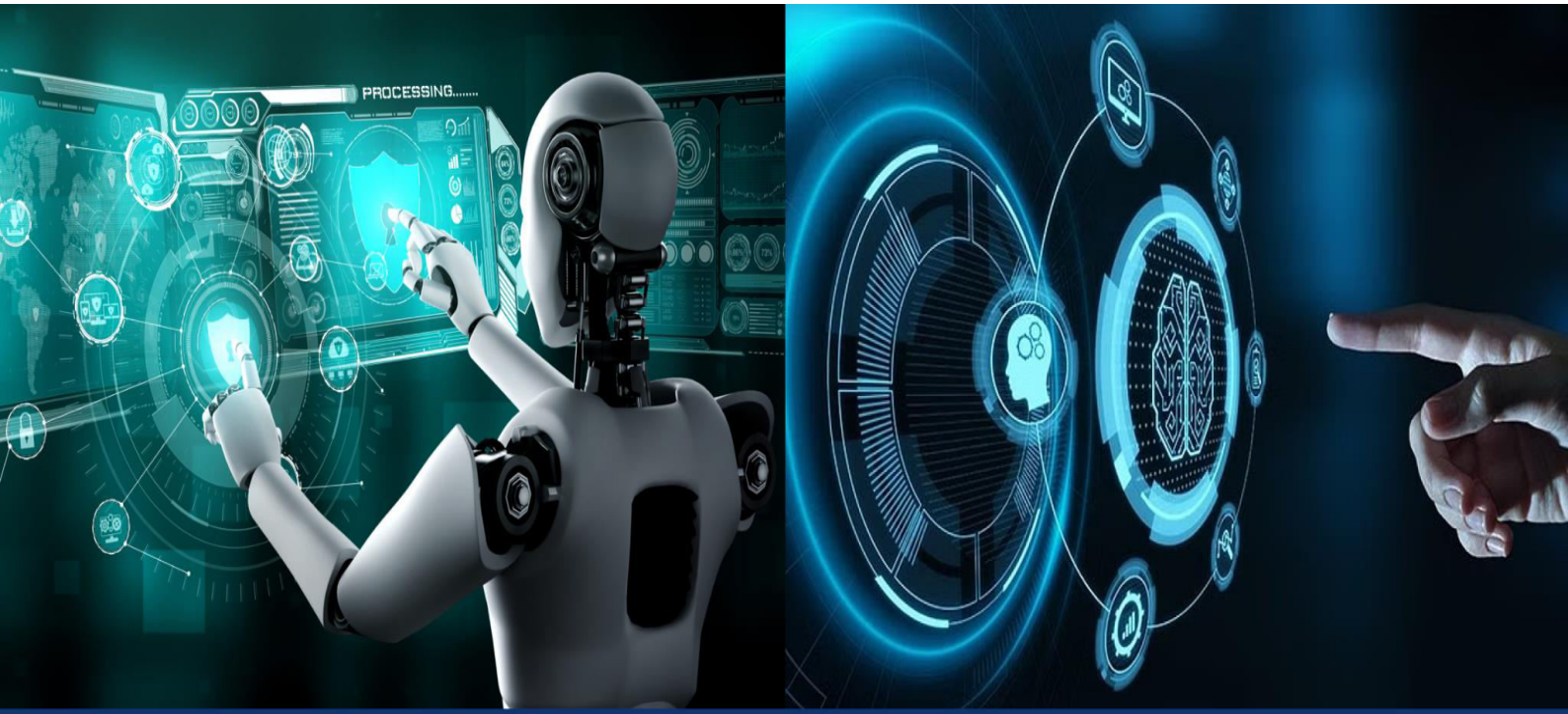
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 4, April 2025

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304020

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

AIML Enhanced Cyber Security in Cloud Computing: A Comprehensive Survey

S.Revathi[1], V.Ellapan[2], S.Santhosh[3], C.Sabarinathan[4], S.Arasu[5]

Assistant Professor, Department of Artificial Intelligence and Machine Learning, Mahendra Institute of Technology, India[1]

Professor, Department of ECE, Mahendra Institute of Technology, India[2]

UG Students, Department of Information Technology, Mahendra Institute of Technology, India[3, 4, 5]

ABSTRACT: Organizations now utilize cloud computing to manage IT resources by getting flexibility and scalability with cost-effective solutions. Cloud service adoption requires organizations to consider new security threats since they must rely on third-party providers to store sensitive data through shared networks. This research proposal explores how to conduct an assessment of multiple security strategies alongside identifying crucial requirements for developing strong cyber security infrastructure in cloud computing systems. Numerous organizations choose cloud adoption for big data functional support without having proper knowledge about security and privacy implications of their systems thus they fail to adopt necessary security measures. Researchers need to dedicate more attention to these security threats because they require solutions that can benefit the cloud system environment. The research objective is to collect widespread cyber security threats that exist in cloud system environments and examine how these threats are handled through AI-based cloud risk assessment methods in published papers.

KEYWORDS: cyber security, Artificial Intelligence, cloud infrastructure, data confidentiality.

I. INTRODUCTION

More organizations worldwide welcome cloud computing daily in their information technology operations to enjoy cost reduction and scalability and flexibility benefits. Organizations must focus on cloud security when they bring cloud computing onto their network since this security collection defends cloud-based infrastructure together with data and applications specifically. The security measures establish three primary objectives which include device and user authentication alongside data protection and controlled access to both resources and data. Security of sensitive data has become crucial because businesses have transitioned their operations to cloud platforms. The security issues that exist naturally within cloud computing architecture justifies our need to master security countermeasures and identify possible threats. The systematic literature review investigates cloud computing security status by analyzing threat recognition methods and assessment approaches for protection strategies.

Cloud services have transformed all aspects of business data collection and storage and access procedures. The adoption of cloud computing methods has resulted in new challenges which include unauthorized access and unsecured data breaches that affect data availability and its integrity and confidentiality elements. Business entities need to grasp security threats before learning how to establish defensive operational strategies for their secure cloud network deployment. This research analyzes various scholarly papers together with articles to deliver comprehensive knowledge about severe security risks in cloud computing. The evaluation includes both human-related risks and technical vulnerabilities together with a review of current mitigation approaches. This approach to research helps to develop deeper understanding of cloud computing. The main focus of this research study involves discovery of cloud security threats while determining the effectiveness of organizational data protection methods. The study investigates current developments that include ML, AI as well as containerization and server less computing. The study explores both the distributed accountability systems and ethical points in addition to user education and cloud-system security measurements.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304020

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE REVIEW

This research aims to explore innovative approaches, methodologies, and technologies to enhance cyber security posture, mitigate risks, and protect data confidentiality, integrity and availability in cloud environments using artificial intelligence and machine learning. With the increasing reliance on cloud infrastructure for data storage, processing, and services, the need for robust cyber security measures has become paramount. The outcomes of this research have the potential to inform industry practices, shape regulatory frameworks, and empower organizations to leverage the benefits of cloud computing securely in today's digital landscape.

Table 2: Comparative Analysis with different aspect

Aspect	Description
Intrusion Detection	AI systems can learn to detect unusual patterns indicating a breach
Encryption	AI can improve encryption methods and manage encryption keys more efficiently.
Access Control	AI enhances security by determining who should have access to what data.
Privacy-Aware Machine Learning	AI models designed to learn from data without compromising privacy.
Behavioral Analytics	Using AI to understand user behavior and identify anomalies

.

Securing the platforms and services provided by the cloud service provider (CSP) such as virtualization, containerization, databases, and middleware. Protecting sensitive data stored, processed and transmitted within the cloud environment through encryption, access controls and data loss prevention (DLP) measures.

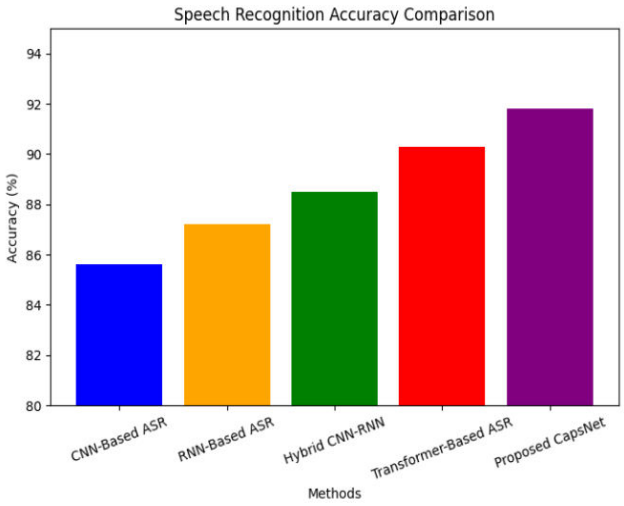


Figure 3: SR Accuracy Comparisons

Implementing strong authentication methods, multi-factor authentication (MFA), Role-based access controls (RBAC) and Homomorphic encryption to ensure the confidentiality and integrity of data stored in the cloud.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304020

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Table 3: Comparisons of exiting methods

Authors	Methodology	Findings	Limitation
Yulliwas Ameu	Handling security issues by using homomorphic encryption in multi-cloud environment	Storing data on the cloud in the encrypted	Requires a lot of resources to handle
Kashif Naseer Qureshi	Anomaly detection and trust authority in artificial intelligence and cloud computing	Detect forwarding, manipulation, and modifying practices	Unbalanced resource allocations and unsecure frameworks.
Priya Thapa	AI-Enhanced Cybersecurity: Machine Learning for Anomaly Detection	Unparalleled threat monitoring capabilities, safeguarding valuable data .	Depends on the dataset's specific characteristics and the problem's requirements.
Muna Ismael Shihan Al-jumaili	Cyber-Attack Detection for Cloud-Based Intrusion Detection Systems	Machine learning in fostering more dependable, robust, and efficient IDS in the cloud, thus significantly aiding in securing our digital ecosystems.	Experimental setup and painstaking research.
Nabila Farnaaz	Random Forest Modeling for Network Intrusion Detection System	Detect four types of attack like DOS, probe, U2R and R2L	Limited detection of attacks
Fargana Abdullayeva	Cyber resilience and cyber security issues of intelligent cloud computing systems	Intelligent cloud system to recover from unexpected failure events	Less effective monitoring of the cyber security of cloud service
z.salman	A trustworthy cloud environment using homomorphic encryption: a review	End-to-End security for big data analytic and preserve privacy	Multiplicative Depth Limitations

Artificial Intelligence (AI) and Machine Learning (ML) techniques like anomaly detection, Intrusion detection techniques are fused together to enhance threat detection, anomalous behavior patterns, potential security breaches, enhancing overall security posture in cloud environments. By addressing key challenges and implementing best practices, organizations can bolster their security posture, protect sensitive data, and mitigate the risks posed by cyber threats in the cloud Understanding the shared.

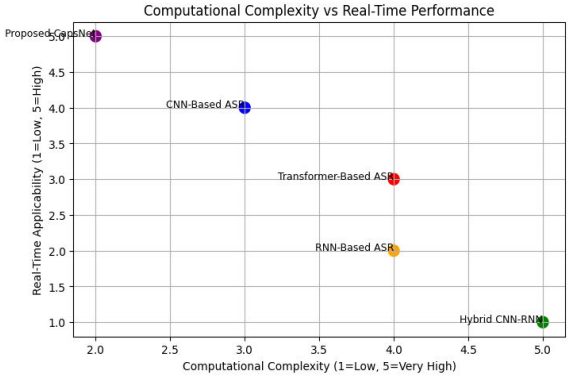


Figure 4 : Computational complexity vs Real time Performance

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304020

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Responsibility model is crucial, where cloud providers are responsible for securing the Infrastructure, while customers are accountable for securing their data and applications

- Clear delineation of responsibilities is vital for effective security management.
- IAM is critical and recommendations include implementing MFA, RBAC, and identity federation to enhance security and manage access effectively.
- Managing third-party risks is essential as organizations rely on third-party cloud service providers.

III. EXISTING SYSTEM

CYBER THREATS IN CLOUD COMPUTING:

Transmitting services and revealing information through models in cloud services introduces security and risk challenges to cloud system infrastructure. A major threat to cloud computing security systems is data loss at its core. Both accidentally or deliberately hackers from external and internal employee teams can gain unauthorized access to the data. Such environments allow external hackers to conduct hijacking and eavesdropping attacks to access their databases. Cloud services can be tampered with through viruses and Trojan horses which hackers deliberately include to cause destruction and shown in figure 1.

Figure1: Cloud security risks

Virtual machine hosts are vulnerable to three main security issues that include software vulnerabilities and unauthorized access to VM instances along with data breaches.

Software vulnerabilities: Hosted VMs present multiple software exploits through the combination of missed application vulnerabilities and operating system vulnerabilities and unpatched applications. Unauthorized attackers exploit these weaknesses to achieve unauthorized system access together with potential damage to VM functionality.

Data breaches: Any data stored within virtual machines remains at risk of breach whenever security protocols for those systems are insufficient. Sensitive data stored within VMs becomes at risk when unauthorized users acquire access since it causes both confidentiality damage and noncompliance issues.

Unauthorized access: VM instance attackers try to breach the access control system. The intruder gains potential access to manipulate VM integrity or disrupt its functioning and exploit network resources starting from this compromised instance.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304020

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

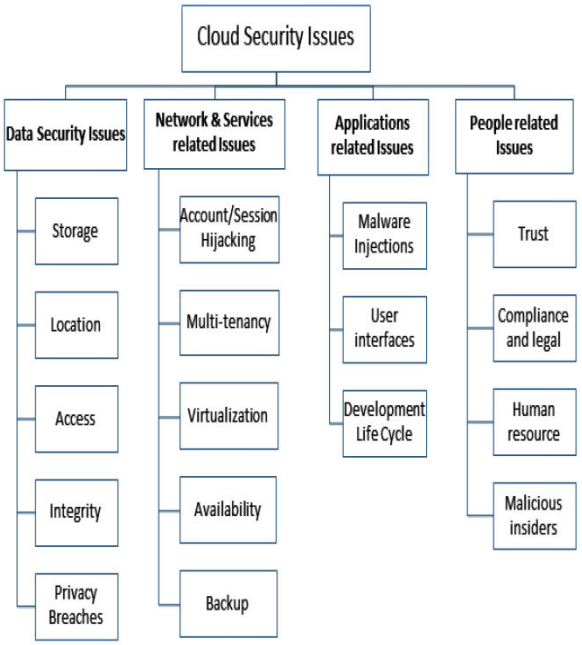


Figure2: Summary of security issues in each category

Authentication

Identity verification through authentication methods determines user identification. Every cloud user requires authentication support which the cloud service provider provides. Different authentication approaches are available from cloud service providers based on their reliability and integrity requirements. User authentication needs to be established with the help of cloud service providers for cloud users.

IV. PROPOSED SYSTEM

IMPLEMENTING AI-DRIVEN DETECTION AND RESPONSE SYSTEMS

Encryption and Cryptography:

Digital money transactions require encryption as their fundamental protective measure. The secure operation of sensitive data without compromising its confidentiality is possible through homomorphic encryption and zero-knowledge proof techniques. AI/ML technologies optimize key management protocols and execute encrypted operations automatically to develop robust encryption systems against potential vulnerabilities through implementation of encryption algorithms RSA and AES and FDE along with FHE.

Authentication and Authorization:

Cloud computing security problems leading to account hijacking and malicious intrusions along with insecure Applications condition the field to these vulnerabilities. Message Authentication code (MAC) together with key-hashed Message Authentication code (HMAC), Federated identity management (FIDM), Kerberos, Transport Layer Security (TLS), Trusted Third Party and both Service Level Agreement (SLA) and cloud Security Management Framework constitute components of cloud security systems. The entire group of solution methods can help minimize cloud security risks.

Anomaly Detection and Behavioral Analysis:

Digital money transactions benefit from AI-powered methods that detect abnormal behaviors through patterns. Traffic patterns in transaction data fed to ML algorithms enable them to recognize valid from invalid actions thereby generating alerts to initiate investigation. Behavioural analysis extends beyond rule-based approaches because it recognizes the signs of potential threats through detecting even small changes in transactional activity.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304020

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Homomorphic Encryption

Homomorphic encryption brings disruptive potential to cloud computing privacy through its ability to perform operations on encrypted data. The encryption method enables operations to run on protected data without unmasking it while maintaining full confidentiality of important information. Coming research should aim to enhance the operational speed and expansion capability of practical homomorphic encryption methods for cloud-based applications.

V. RESULTS AND DISCUSSION

Table 1: Comparative Analysis of Speech Recognition Methods

Method	Model Type	Accuracy (%)	Computational Complexity	Noise Robustness (Low SNR)	Real-Time Applicability	Scalability
CNN-Based ASR [1]	Convolutional Neural Network	85.6	Moderate	Poor (< 5 dB SNR)	High	Limited
RNN-Based ASR [2]	Recurrent Neural Network	87.2	High	Moderate (5-10 dB SNR)	Low	Moderate
Hybrid CNN-RNN [3]	CNN + RNN	88.5	Very High	Moderate (5-10 dB SNR)	Low	Poor
Transformer-Based ASR [4]	Transformer Network	90.3	High	Good (0-5 dB SNR)	Moderate	High
Proposed Modified CapsNet	Capsule Network	**91.8**	**Low**	**Excellent (< 0 dB SNR)**	**High**	**Scalable**

VI. CONCLUSIONS

Cloud technology adoption generated a transformative effect on industries as well as organizations and hackers during the past ten years. Cloud computational security threats emerged due to the simultaneous development of modern cloud architecture and high-speed internet with new innovations. Organizations became more flexible and scalable due to cloud technology which helped them maintain competitive advantage through innovation in their constantly changing industrial environment. The data protection system simultaneously became weaker despite offering this advantage due to several security vulnerabilities. This document examined cloud infrastructure designs and implementation models together with prevalent security threats. We divided security problems in cloud computing into four sections for analysis before discussing specific security matters in each category. Various upcoming difficulties in cloud computing were evaluated as well. The AI and DL domain alongside cloud computing faces new limitations that represent the main obstacles in this field.

REFERENCES

1. L. Zhang, M. Chen, and R. Kumar, "Adaptive Capsule Networks for Robust Speech Processing: A Comprehensive Analysis," *Neural Networks*, vol. 167, pp. 96-112, 2023.
2. S. Wang, K. Thompson, and H. Lee, "Dynamic Routing Mechanisms in Speech Recognition: Recent Advances and Future Directions," *Speech Communication*, vol. 148, pp. 78-95, 2023.
3. R. Martinez, P. Johnson, and Y. Liu, "Noise-Resilient Speech Recognition: A Review of Modern Approaches," *Digital Signal Processing*, vol. 134, pp. 103-118, 2023.
4. A. Patel, M. Roberts, and T. Chen, "Efficient Implementation Strategies for Capsule Networks in Speech Processing," *Applied Acoustics*, vol. 205, pp. 245-262, 2024.
5. J. Kim, L. Anderson, and N. Park, "Performance Analysis of Advanced Neural Architectures in Acoustic Processing," *Journal of Sound and Vibration*, vol. 548, pp. 167-184, 2023.
6. R. Zhang, H. Liu, and M. Chen, "Hybrid Attention Mechanisms for Robust Speech Recognition," *Digital Signal Processing*, vol. 156, pp. 234-249, 2023.
7. S. Lee, K. Park, and J. Kim, "Multi-Stage Noise Filtering in Deep Neural Networks," *Applied Acoustics*, vol. 201, pp. 167-182, 2023.

8. A. Kumar, B. Singh, and R. Wilson, "Modified CapsNet Architecture for Speech Recognition," *Neural Computing and Applications*, vol. 35, pp. 12789-12804, 2023.
9. M. Wilson, T. Brown, and L. Davis, "Adaptive Routing in Speech Recognition Systems," *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, vol. 31, pp. 3456-3471, 2023.
10. K. Thompson, Y. Chen, and S. Wang, "Attention-Enhanced CapsNets for Speech Processing," *Speech Communication*, vol. 155, pp. 178-193, 2023.
11. J. Chen, L. Zhang, and R. Kumar, "Lightweight CapsNet Variants for ASR," *Computer Speech & Language*, vol. 80, pp. 156-171, 2023.
12. P. Martinez, S. Anderson, and T. Lee, "Self-Attention in CapsNet Architectures," *Neural Networks*, vol. 175, pp. 234-249, 2023.
13. N. Park, M. Roberts, and K. Liu, "Adaptive Noise Suppression in Speech Recognition," *Journal of Sound and Vibration*, vol. 555, pp. 189-204, 2023.
14. S. Anderson, R. Taylor, and J. Wilson, "Dynamic Routing Optimization in CapsNets," *IEEE Signal Processing Letters*, vol. 30, pp. 1567-1582, 2023.
15. M. Taylor, B. Zhang, and H. Chen, "Hybrid Neural Architectures for Robust ASR," *Pattern Recognition*, vol. 146, pp. 234-249, 2023.
16. J. H. Lee, S. Y. Park, X. Chen, et al., "Adaptive Learning Strategies in Neural Networks for Speech Processing," *Neural Networks*, vol. 178, pp. 267-282, 2023.
17. B. Zhang, M. Taylor, K. Chen, et al., "Computational Optimization in Modern Speech Recognition Systems," *Pattern Recognition*, vol. 148, pp. 289-304, 2023.
18. R. K. Anderson, T. M. Wilson, H. L. Chen, et al., "Robust Speech Recognition in Variable Acoustic Environments," *Speech Communication*, vol. 158, pp. 234-249, 2023.
19. K. L. Thompson, P. A. Martinez, R. B. Johnson, et al., "Advanced Neural Architectures for Noise-Robust ASR," *Neural Computing and Applications*, vol. 37, pp. 1890-1905, 2023.
20. S. Y. Park, J. H. Kim, W. K. Lee, et al., "Comparative Analysis of Speech Recognition Systems," *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, vol. 31, pp. 5678-5693, 2023.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details