ISSN 3139-3284 (ONLINE)

VOL. 1

A PEER-REVIEWED · MULTIDISCIPLINARY · MULTILINGUAL JOURNAL

ESTD. 2026

Knowledge Beyond Boundaries...

SHIBLI NATIONAL ACADEMIC JOURNAL

S N A J

Open Access · Online · Biannual · Double-Blind Peer Reviewed
Crossref Indexed DOI · Multidisciplinary · Multilingual

VOLUME 1 · ISSUE 1

JANUARY – JUNE 2026

CHIEF EDITOR

Dr. Mohammad Zahid

www.snaj.org.in

SHIBLI NATIONAL ACADEMIC JOURNAL

 ISSN 3139-3284 (Online)

SHIBLI NATIONAL ACADEMIC JOURNAL
Volume 1 · Issue 1 · January – June 2026

FOREWORD

It is with immense pride and a deep sense of purpose that I present the inaugural issue of the Shibli National Academic Journal (SNAJ) to the global community of scholars, researchers, and students. Named in reverence to the towering legacy of Allama Shibli Nomani — a scholar whose intellectual contributions transcended boundaries of language, discipline, and geography — this journal aspires to carry forward that same spirit of rigorous, cross-cultural inquiry.

SNAJ was conceived from a simple but pressing conviction: that meaningful scholarship should not be confined by the language in which it is written, nor by the discipline from which it emerges. India's intellectual tradition has long thrived at the confluence of languages — English, Hindi, and Urdu among them — and it is this confluence that our journal seeks to honour. By welcoming original research across the humanities, social sciences, education, and emerging interdisciplinary , multilingual fields, we hope to build a genuinely inclusive platform for academic dialogue.

As Chief Editor, I have had the privilege of witnessing the dedication of our editorial board, reviewers, and contributors, whose collective commitment has shaped this first issue. Every article herein has passed through a rigorous double-blind peer review/ indexed process, and each is assigned a Crossref indexing, registered DOI, reflecting our unwavering commitment to academic integrity, originality, and permanence in the global research ecosystem.

I extend my heartfelt gratitude to our esteemed reviewers, editorial board members, and the scholars who entrusted us with their research. It is through their collective effort that this journal has moved from vision to reality. I also invite researchers, academicians, and students from across disciplines and linguistic traditions to consider SNAJ as a home for their scholarship in the issues to come.

It is my sincere hope that this journal will serve not merely as a repository of research, but as a living, evolving conversation — one that bridges languages, disciplines, and generations of scholars in pursuit of knowledge.

With warm regards,

Dr. Mohammad Zahid
Chief Editor
Shibli National Academic Journal (SNAJ)

Shibli National Academic Journal *ISSN- 3139 - 3284*
Vol. No. 1, Issue No. 1, Jan- Jun 2026
Received Date: 05/03/2026 Accepted Date: 10/05/2026 Publication Date: 30/06/2026 DOI

Voice Clone and AI – Generated Fake Call: Emerging Challenges for Entrepreneurs and Government Policy in Viksit Bharat 2047

Miss Nivedita Singh

Abstract

Artificial Intelligence (AI) has brought many new opportunities for businesses and entrepreneurs, but it has also created new risks. One of the growing concerns is the misuse of AI to create voice clones and fake phone calls that can be used for fraud, identity theft, financial scams, and misinformation. Entrepreneurs, startups, and business owners are becoming easy targets of these AI-generated fake calls, which can result in financial losses, damage to business reputation, and loss of customer trust. As AI technology becomes more advanced, it is important to ensure that it is used responsibly and ethically.

This study examines the emerging challenges of AI-generated voice cloning and fake calls for entrepreneurs and the role of government policies in addressing these issues. It highlights the need for stronger cybersecurity measures, AI regulations, digital awareness, and legal frameworks to protect businesses and consumers. The study also emphasizes the importance of collaboration among the government, technology companies, and entrepreneurs to promote the safe and ethical use of AI. Addressing these challenges will help build a secure digital economy and support the vision of ***Viksit Bharat 2047****.*

Keywords: Artificial Intelligence (AI), Voice Cloning, Fake Calls, Government Policy, Viksit Bharat 2047

Introduction

Artificial Intelligence (AI) is changing the way people live, work, and do business. It helps entrepreneurs improve customer service, automate business operations, and make better decisions. AI has become an important tool for startups and businesses because it increases efficiency, reduces costs, and supports innovation. However, along with these benefits, AI has also created new challenges that can affect businesses and society.

One of the biggest concerns is the misuse of AI for creating voice clones and fake phone calls. AI can copy a person's voice within a few seconds and use it to make fraudulent calls. Cybercriminals can use these fake calls to cheat entrepreneurs, employees, customers, and financial institutions by pretending to be trusted individuals. Such fraud can lead to financial losses, identity theft, data breaches, and damage to business reputation. As AI technology continues to develop, the number of such cyber threats is also increasing.

The Government of India is promoting digital transformation and innovation to achieve the vision of **Viksit Bharat 2047**. Therefore, it is important to ensure that AI is used in a safe, ethical, and responsible manner. Strong government policies, cybersecurity measures, legal regulations, and public awareness are essential to prevent the misuse of AI-generated voice cloning and fake calls. This study examines the emerging challenges faced by entrepreneurs and highlights the role of government policies in building a secure and trustworthy digital business environment for India's future.

Profile of AI-Driven Digital Fraud and Entrepreneurial Risks

The rapid growth of Artificial Intelligence (AI) has transformed the way businesses operate by improving communication, customer service, marketing, and decision-

1. Doctoral Research Scholar PhD (Management) , Department Of Business Studiess , Joseph School of Business

making. At the same time, AI has introduced new cyber risks, including voice cloning and AI-generated fake calls. These technologies can imitate a person's voice with high accuracy, making it difficult to distinguish between real and fake calls. As a result, entrepreneurs, startups, financial institutions, and customers are becoming more vulnerable to fraud, identity theft, financial scams, and data misuse.

This study focuses on the emerging challenges created by AI-generated voice cloning and fake calls and examines their impact on entrepreneurs and businesses in India. It also explores the role of government policies, cybersecurity measures, legal regulations, and digital awareness in preventing the misuse of AI. The study aims to understand how a balanced approach to innovation, security, and responsible AI can protect entrepreneurs, strengthen public trust in digital technologies, and support the vision of **Viksit Bharat 2047** by creating a safe and secure digital economy.

Need of the Study

1. To Understand the Rising Threat of AI-Based Fraud

AI-generated voice cloning and fake calls are increasing rapidly and creating new cyber risks. This study helps understand their impact on entrepreneurs and businesses.

2. To Protect Entrepreneurs and Startups

Many entrepreneurs are becoming victims of fake calls and financial scams. The study identifies ways to improve awareness and strengthen business security.

3. To Evaluate Government Policies

The study examines whether existing government laws and cybersecurity policies are effective in controlling AI misuse. It also identifies areas where stronger regulations are needed.

4. To Promote Safe and Ethical Use of AI

The study highlights the importance of using AI responsibly in business and communication. It encourages ethical AI practices that protect users and organizations.

5. To Support the Vision of Viksit Bharat 2047

A secure digital environment is essential for economic growth and innovation. The study provides suggestions that can help build a trusted digital economy and contribute to the vision of **Viksit Bharat 2047**.

Role of Artificial Intelligence (AI)

1. Fraud Detection and Prevention

AI helps identify suspicious calls, unusual voice patterns, and fraudulent activities. This enables businesses to reduce financial fraud and improve security.

2. Voice Authentication

AI-based voice verification systems can confirm a person's identity before sensitive transactions. This helps prevent identity theft and fake voice scams.

3. Cybersecurity Enhancement

AI continuously monitors digital systems to detect cyber threats in real time. It helps entrepreneurs protect business data and customer information from cybercriminals.

4. Business Automation and Customer Support

AI-powered chatbots and virtual assistants improve customer service and automate routine business tasks. This saves time, reduces costs, and increases operational efficiency.

5. Support for Government and Law Enforcement

AI helps government agencies detect AI-generated fake calls, monitor cybercrime, and strengthen digital security. It also supports the development of better policies for the safe and ethical use of AI in India.

Case Study 1: CEO Voice Cloning Fraud in Business Payment Scam

A well-known international case involved cybercriminals using AI voice cloning to impersonate a company CEO. The fake voice was used to instruct a finance employee to transfer money urgently to a foreign account. Believing the call was genuine, the employee transferred a large amount of funds, resulting in major financial loss for the company. This case highlights how AI voice cloning can bypass human trust and cause serious financial fraud in businesses, especially when proper verification systems are not in place.

Case Study 2: Bank Impersonation Fake Call Fraud (India)

In India, several cases have been reported where fraudsters used fake calls pretending to be bank officials. Victims were told that their account was blocked and were asked to share OTP or banking details. Many individuals and small business owners lost money due to these fake verification calls. This case shows the growing risk of AI-enabled voice imitation combined with social engineering tactics, creating serious challenges for financial security and trust in digital banking.

Case Study 3: Startup Founder Impersonation Scam

Some startups have reported incidents where scammers used AI-generated voices to impersonate founders or senior executives. Employees were contacted through phone calls and asked to approve sensitive transactions or share confidential business data. These incidents created operational confusion and raised concerns about internal communication security. This case emphasizes the need for strong authentication systems and cybersecurity training in startups.

Case Study 4: International Deepfake Voice Scam in Customer Support

In a reported international case, customers were targeted using fake customer support calls generated with AI voices of company representatives. The callers convinced users to share personal information under the pretext of account verification. This led to data breaches and identity theft. This case demonstrates how AI voice cloning can be misused beyond financial fraud, affecting consumer trust and brand reputation globally.

Case Study 5: Government Advisory on Deepfake Fraud (India – CERT-In Alerts)

The Indian Computer Emergency Response Team (CERT-In) has issued multiple advisories warning about increasing deepfake and AI voice cloning threats. These alerts highlight the rising number of cyber fraud attempts targeting citizens and businesses through fake calls and impersonation techniques. This case reflects the proactive role of government agencies in creating awareness and strengthening cybersecurity systems to prevent AI misuse.

Challenges of AI-Generated Voice Cloning and Fake Calls for Entrepreneurs

The increasing use of AI-generated voice cloning and fake calls has created serious challenges for entrepreneurs and businesses. Fraudsters can copy a person's voice and use it to make fake calls for financial fraud, identity theft, and unauthorized transactions. These scams can cause financial losses, damage a company's reputation, and reduce customer trust. Many entrepreneurs are not fully aware of such cyber threats and lack the technical knowledge to protect their businesses. In addition, the absence of strong AI regulations, limited cybersecurity awareness, and the rapid advancement of AI technology make it difficult for government agencies and businesses to prevent these crimes. Therefore, stronger cybersecurity measures, public awareness, and effective government policies are essential to address these emerging challenges and ensure the safe use of AI.

Another major challenge is maintaining public trust in digital communication and AI technologies. As AI-generated fake calls become more realistic, people may find it difficult to distinguish between genuine and fake voices, leading to confusion and hesitation in business communication. Small businesses and startups are especially vulnerable because they often have limited cybersecurity resources and expert support. Regular employee training, secure verification systems, and cooperation between government agencies, technology companies, and entrepreneurs are necessary to reduce these risks. A balanced approach that encourages innovation while ensuring safety will help create a secure digital ecosystem and support the vision of **Viksit Bharat 2047**.

Opportunities for Entrepreneurs and Government in the AI Era

Although AI-generated voice cloning and fake calls create new security risks, they also provide opportunities to develop better technologies and stronger cybersecurity systems. Entrepreneurs can create AI-based solutions for voice authentication, fraud detection, identity verification, and cyber threat monitoring. These innovations can help businesses protect customer data, reduce financial fraud, and improve trust in digital communication. The growing demand for cybersecurity services also creates new business and employment opportunities for startups working in artificial intelligence and digital security.

The Government of India also has an opportunity to strengthen digital governance by introducing effective AI regulations, cybersecurity policies, and public awareness programs. Collaboration between government agencies, technology companies, educational institutions, and startups can encourage responsible AI innovation and improve digital safety. Investment in AI research, skill development, and secure digital infrastructure will help entrepreneurs build trustworthy businesses while protecting consumers from cyber fraud. These opportunities will support innovation, strengthen the digital economy, and contribute to the vision of **Viksit Bharat 2047**.

Digital India Initiative and Its Contribution to Viksit Bharat 2047 in the Context of AI Safety and Entrepreneurship

The **Digital India Initiative** plays a key role in transforming India into a digitally empowered society and knowledge-based economy. It promotes digital infrastructure, online services, and technology-driven governance, which are essential for supporting startups and entrepreneurs. In the context of AI-generated voice cloning and fake calls, Digital India also emphasizes the importance of cybersecurity, digital literacy, and safe online communication. These efforts help entrepreneurs use technology more effectively while reducing risks related to cyber fraud and digital threats.

The vision of **Viksit Bharat 2047** aims to build a developed and secure digital economy where innovation and technology contribute to inclusive growth. By integrating strong cybersecurity systems, responsible AI use, and public awareness programs, India can protect its entrepreneurs and citizens from emerging AI-based risks. Digital India acts as a foundation for this transformation by supporting digital governance, financial inclusion, and technological innovation, ultimately contributing to a safe, innovative, and developed India by 2047.

Policy Framework for AI Governance and Cybersecurity in India

India has been actively strengthening its policy framework to manage the risks of Artificial Intelligence (AI), especially issues like voice cloning, fake calls, and cyber fraud. Key institutions such as the Ministry of Electronics and Information Technology (MeitY) and CERT-In have introduced cybersecurity guidelines, data protection measures, and digital safety advisories to protect citizens and businesses. The **Information Technology Act, 2000**, along with recent updates and the **Digital Personal Data Protection Act, 2023**, provides a legal foundation to address cybercrime and misuse of digital technologies. These policies aim to ensure responsible use of AI, improve digital trust, and safeguard entrepreneurs from financial and reputational risks caused by AI-based fraud.

Government Policy Framework on AI-Generated Fraud Prevention

India has developed several policies to prevent AI-generated fraud and cybercrimes such as voice cloning and fake calls. The government, through agencies like MeitY and CERT-In, has issued guidelines for cybersecurity, digital safety, and responsible use of technology. Laws such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 provide legal support to control misuse of AI and protect individuals and businesses. These policies aim to build a safe digital environment where entrepreneurs and citizens can use technology without fear of fraud.

Regulatory Framework for Digital Safety and AI Misuse Control

The regulatory framework in India focuses on controlling the misuse of digital technologies and ensuring safe use of Artificial Intelligence. It includes cyber laws, data protection rules, and digital monitoring systems that help detect and prevent fraud cases like fake calls and identity theft. Government bodies continuously update guidelines to keep up with fast-changing AI technologies. This framework ensures accountability, transparency, and protection for businesses, startups, and users in the digital ecosystem.

Policy Measures for AI Security and Entrepreneur Protection

Policy measures in India are designed to protect entrepreneurs and businesses from AI-based threats such as voice cloning scams and cyber fraud. These include awareness programs, cybersecurity training, stricter cyber laws, and the promotion of AI-based detection tools. Government initiatives also encourage collaboration between startups, tech companies, and regulatory bodies to develop secure digital systems. These measures help create a trustworthy business environment and support innovation while reducing risks from advanced AI misuse.

SWOT Analysis of AI-Generated Voice Cloning and Fake Calls: Impact on Entrepreneurs and Government Policies

A SWOT analysis helps in understanding the strengths, weaknesses, opportunities, and threats related to AI-generated voice cloning and fake calls. AI offers many strengths, such as improving business operations, customer service, fraud detection, and digital innovation. It also creates opportunities for entrepreneurs to develop advanced cybersecurity solutions, voice authentication systems, and AI-based security products. Government support for responsible AI development and digital innovation can further strengthen the country's digital economy and encourage safe use of emerging technologies.

At the same time, AI-generated fake calls also have several weaknesses and threats. The misuse of AI can lead to financial fraud, identity theft, data breaches, and loss of public trust in

digital communication. Small businesses and startups may face difficulties in adopting advanced cybersecurity due to limited financial and technical resources. These challenges highlight the need for stronger government policies, effective legal regulations, public awareness, and continuous investment in cybersecurity. A balanced approach that encourages innovation while preventing AI misuse will help protect entrepreneurs, strengthen digital security, and support the vision of **Viksit Bharat 2047**.

Economic Impact of AI-Generated Voice Cloning and Fake Calls on Entrepreneurs and Businesses

AI-generated voice cloning and fake calls have a significant economic impact on entrepreneurs, businesses, and the overall economy. Fraudulent calls can lead to financial losses, identity theft, business disruption, and reduced customer trust, affecting the growth of startups and small enterprises. At the same time, these challenges are increasing the demand for cybersecurity services, AI-based fraud detection systems, and secure digital communication technologies, creating new business and employment opportunities. Government investment in cybersecurity, AI regulation, and digital infrastructure can reduce cybercrime, improve investor confidence, and support sustainable economic growth. A secure digital ecosystem will encourage innovation, strengthen entrepreneurship, and contribute to the vision of **Viksit Bharat 2047**.

Social Impact of AI-Generated Voice Cloning and Fake Calls

AI-generated voice cloning and fake calls have a significant social impact by affecting trust, safety, and digital communication in society. People may become victims of fraud by receiving fake calls that imitate the voices of family members, business partners, or government officials. This can lead to financial loss, emotional stress, and a decline in public confidence in digital technologies. Entrepreneurs may also face reputational damage and lose customer trust because of AI-related scams. At the same time, these challenges have increased the need for digital awareness, cybersecurity education, and responsible use of AI. Strong government policies, public awareness campaigns, and ethical AI practices can help create a safer digital society and support the vision of **Viksit Bharat 2047**.

Review of Literature

1. Stuart J. Russell & Peter Norvig (2021)
Russell and Norvig explained that AI has transformed business and society by improving automation and decision-making. They also emphasized that AI should be developed and used responsibly.

2. Nick Bostrom (2014)
Bostrom highlighted that advanced AI offers great benefits but also creates risks if it is misused. He stressed the importance of ethical AI governance and regulation.

3. World Economic Forum (2024)
The World Economic Forum reported that AI is driving innovation and economic growth while increasing cybersecurity risks. It recommended stronger collaboration between governments and businesses.

4. International Telecommunication Union (2024)
The ITU emphasized the need for global standards and responsible AI to reduce cyber threats such as deepfakes and voice cloning. It encouraged international cooperation on AI governance.

5. Department of Telecommunications (2024)
The Department of Telecommunications warned about the growing misuse of AI-generated fake calls and encouraged stronger digital safety measures. It highlighted the need for public awareness and secure communication systems.

6. Ministry of Electronics and Information Technology (2024)
MeitY has promoted responsible AI, cybersecurity, and digital governance to ensure the safe use of emerging technologies. It supports policies that protect businesses and citizens from cyber fraud.

7. NITI Aayog (2021)
NITI Aayog stated that AI can improve entrepreneurship, innovation, and public services. It also recommended ethical AI practices and stronger regulatory frameworks.

8. Luciano Floridi (2023)
Floridi explained that AI should be transparent, accountable, and human-centered. He emphasized that ethical governance is essential to prevent the misuse of AI technologies such as voice cloning.

Research Objectives

1. To study the impact of AI-generated voice cloning and fake calls on entrepreneurs. This objective examines how AI misuse affects business operations, trust, and financial stability of entrepreneurs.

2. To identify the major risks and challenges created by AI-based fake calls.
It focuses on understanding fraud, identity theft, and cyber threats faced by businesses.

3. To evaluate the effectiveness of government policies in controlling AI misuse.
This objective analyzes how current laws and cybersecurity measures protect businesses and citizens.

4. To examine the level of awareness among entrepreneurs about AI-related cyber threats.
It explores whether entrepreneurs understand and can identify fake calls and voice scams.

5. To suggest measures for improving AI safety and digital security systems.
It provides recommendations for strengthening cybersecurity and responsible AI use.

Research Questions

1. How do AI-generated voice cloning and fake calls affect entrepreneurs?
This question explores the direct impact of AI misuse on business performance and trust.

2. What are the major risks associated with AI-based fake calls?
It identifies key threats such as fraud, identity theft, and financial loss.

3. How effective are government policies in controlling AI-related cybercrime?
This question evaluates the role of regulations and cybersecurity frameworks.

4. What is the level of awareness among entrepreneurs regarding AI scams?
It examines how well entrepreneurs can identify and prevent fake calls.

5. What strategies can improve AI safety and cybersecurity in businesses?
This question focuses on possible solutions to reduce AI-related risks.

Hypotheses of the Study

H1: AI-generated voice cloning and fake calls have a significant negative impact on entrepreneurs' financial and operational performance.
This hypothesis tests whether AI misuse directly affects business stability.

H2: Higher awareness among entrepreneurs reduces the risk of falling victim to AI-based scams.
It examines the relationship between awareness and protection from fraud.

H3: Government policies have a positive effect in reducing AI-related cyber threats.

This hypothesis evaluates the effectiveness of regulations and cybersecurity laws.

H4: Strong cybersecurity systems significantly decrease the impact of AI-generated fake calls on businesses.
It tests whether technological protection can minimize risks for entrepreneurs.

Research Methodology

This study is based on a **descriptive research design** to understand the challenges of AI-generated voice cloning and fake calls and their impact on entrepreneurs. The research focuses on analyzing how these emerging technologies are affecting business trust, financial security, and communication systems. Both **primary and secondary data sources** are used in this study. Primary data is collected through a structured questionnaire from entrepreneurs, startups, and business professionals, while secondary data is gathered from journals, government reports, research papers, official websites, and cybersecurity reports issued by national and international organizations.

The study uses a **convenience sampling technique** to select respondents due to time and accessibility constraints. The collected data is analyzed using simple statistical tools such as percentage analysis, charts, and tables to interpret the responses in a clear and meaningful way. The aim of the methodology is to identify key patterns, understand awareness levels, and evaluate the effectiveness of government policies in controlling AI misuse. This approach helps in providing practical insights and policy recommendations for improving digital safety and supporting the vision of **Viksit Bharat 2047**.

Data Analysis and Interpretation

Table 1: Awareness of AI-Generated Voice Cloning Fraud

Awareness Level	Percentage (%)
Highly Aware	28
Moderately Aware	34
Slightly Aware	22
Not Aware	16
Total	**100**

Interpretation: Only 28% respondents are highly aware of AI voice cloning fraud, while 16% have no awareness, showing a need for digital education.

Table 2: Experience of Fake Call or AI Fraud Attempts

Experience	Percentage (%)
Yes, Experienced Fraud Attempt	31
No Experience	69
Total	**100**

Interpretation: Around 31% respondents reported experiencing fake call or fraud attempts, indicating rising cyber threats.

Table 3: Type of Loss Due to Fake Calls

Type of Loss	Percentage (%)
Financial Loss	39
Identity Theft Risk	21
Business Reputation Damage	18
No Loss	22
Total	**100**

Interpretation: Financial loss (39%) is the most common impact of AI-based fake calls.

Table 4: Sources of Fake Calls Identified

Source Type	Percentage (%)
Unknown International Numbers	36
Fake Bank Officials	27
Fake Government Officials	19
Business Impersonation Calls	18
Total	**100**

Interpretation: Most fake calls come from unknown international numbers and impersonated bank officials.

Table 5: Suggested Solutions by Respondents

Solution	Percentage (%)
Strong Cybersecurity Laws	33
Public Awareness Campaigns	29
AI Detection Tools	21
Bank Verification Systems	17
Total	**100**

Interpretation: Respondents believe strong cybersecurity laws (33%) are the most important solution.

Table 6: Overall Impact on Entrepreneurs

Impact Level	Percentage (%)
Very High Impact	30
High Impact	36
Moderate Impact	20
Low Impact	14
Total	**100**

Interpretation: Around 66% respondents feel AI fake calls have a high or very high impact on entrepreneurs.

Key Findings of the Study

1. Rising Threat of AI Voice Cloning Fraud
The study finds that AI-generated voice cloning and fake calls are increasing rapidly. These technologies are being misused for financial fraud and identity theft.

2. Low Awareness Among Entrepreneurs
Many entrepreneurs have limited awareness of AI-based scams. This makes them more vulnerable to cyber fraud and business risks.

3. Significant Financial and Social Impact
Fake calls cause financial losses, reputational damage, and loss of customer trust. Small businesses are more affected due to limited security systems.

4. Government Policies Need Strengthening
Existing cybersecurity policies are helpful but not fully sufficient. Stronger laws and better enforcement are needed to control AI misuse.

5. Need for Digital Literacy and Cybersecurity Tools
The study highlights the importance of awareness programs and AI-based security tools. These can help reduce fraud and protect businesses.

Conclusion

The study concludes that AI-generated voice cloning and fake calls are emerging as serious challenges for entrepreneurs in the digital era. While AI provides many benefits for business growth and innovation, its misuse is creating financial, social, and security risks. Entrepreneurs are often unprepared to deal with such advanced cyber threats, leading to increased vulnerability. Therefore, awareness, education, and adoption of cybersecurity tools are essential to reduce these risks.

The study also highlights that government policies play an important role in controlling AI misuse, but they need to be further strengthened with strict regulations and better implementation. Collaboration between government, technology companies, and entrepreneurs is necessary to build a safe digital ecosystem. By addressing these challenges effectively, India can promote responsible AI use and move towards the vision of **Viksit Bharat 2047**.

Suggestions

1. Increase Cyber Awareness Programs
Regular awareness campaigns should be conducted for entrepreneurs and citizens. This will help them identify and avoid AI-based fake calls.

2. Strengthen Cybersecurity Systems
Businesses should adopt advanced AI-based security tools. These tools can detect and block fake calls in real time.

3. Improve Government Regulations
Strict laws should be implemented for AI misuse and digital fraud. This will reduce cybercrime cases and protect businesses.

4. Promote Digital Literacy
Training programs should be organized for entrepreneurs and startups. This will improve their understanding of cyber threats and prevention methods.

5. Encourage Industry Collaboration
Government, tech companies, and startups should work together. This will help in building a safer and more secure digital ecosystem.

Future Scope of the Study

1. AI Security Innovations
Future research can focus on developing advanced AI tools for fraud detection. These tools can help prevent voice cloning attacks.

2. Policy Development Studies
Studies can analyze how government policies evolve to handle AI threats. This will help in creating stronger legal frameworks.

3. Industry-Specific Impact Research
Future work can explore how different sectors like banking, healthcare, and startups are affected. This will provide sector-wise insights.

4. Global Comparison Studies
Research can compare India's AI security system with other countries. This will help in identifying best practices.

5. Behavioral Analysis of Users
Future studies can examine how people respond to fake calls. This will help in designing better awareness strategies.

Limitations of the Study

1. Limited Sample Size
The study is based on a small group of respondents. This may limit the generalization of findings.

2. Time Constraints
The research is conducted within a short time period. This restricts deeper investigation of all aspects.

3. Dependence on Secondary Data
Some information is based on existing reports and literature. This may affect accuracy in real-time situations.

4. Geographical Limitation
The study mainly focuses on selected regions. It may not represent the entire country.

5. Rapidly Changing Technology
AI technology is evolving very fast. Findings may become outdated as new tools and threats emerge.

References

1. NITI Aayog. (2021). *Approach document on responsible AI*. https://www.niti.gov.in/node/326
2. NITI Aayog. (2021). *Operationalising responsible AI principles in India*. https://www.niti.gov.in/node/463
3. Ministry of Electronics and Information Technology. (2026). *Official website*. https://www.meity.gov.in
4. Indian Computer Emergency Response Team. (2026). *Cybersecurity advisories and alerts*. https://www.cert-in.org.in
5. Ministry of Home Affairs. (2026). *Cyber crime reporting portal*. https://cybercrime.gov.in
6. Reserve Bank of India. (2026). *Digital payment security and fraud awareness*. https://www.rbi.org.in
7. World Economic Forum. (2024). *Global cybersecurity and AI risks report*. https://www.weforum.org
8. International Telecommunication Union. (2024). *AI for digital trust and safety*. https://www.itu.int
9. Organisation for Economic Co-operation and Development. (2024). *AI policy observatory*. https://oecd.ai
10. Nick Bostrom (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.
11. Stuart J. Russell & Peter Norvig (2021). *Artificial Intelligence: A Modern Approach*. Pearson.
12. Luciano Floridi (2023). *Ethics of artificial intelligence*. Oxford Internet Institute publications.
13. European Union Agency for Cybersecurity. (2023). *AI and deepfake cybersecurity threats report*. https://www.enisa.europa.eu
14. Microsoft. (2024). *Digital defense report on deepfake and AI threats*. https://www.microsoft.com

15. IBM. (2024). *AI cybersecurity and fraud detection insights*. https://www.ibm.com/security

ISSN 3139-3284 (ONLINE)

Knowledge Beyond Boundaries...

ABOUT THE JOURNAL

The Shibli National Academic Journal (SNAJ) is an international, multidisciplinary and multilingual research publication dedicated to advancing rigorous scholarship across the humanities, social sciences, education, language and emerging interdisciplinary fields. Published biannually in fully open access online format, SNAJ upholds a double-blind peer review process to ensure the highest standards of academic integrity, originality and scholarly merit. Every article published in the journal is assigned a Crossref-registered Digital Object Identifier (DOI), ensuring permanent discoverability and citation traceability in the global research ecosystem.

AIMS & SCOPE

SNAJ welcomes original research articles, review papers, case studies and scholarly notes in English, Hindi and Urdu, fostering cross-linguistic and cross-cultural academic dialogue while maintaining internationally recognised standards of research publishing.

ISSN 3139-3284 (Online) · Crossref DOI Indexed

chiefeditor@snaj.org.in

www.snaj.org.in