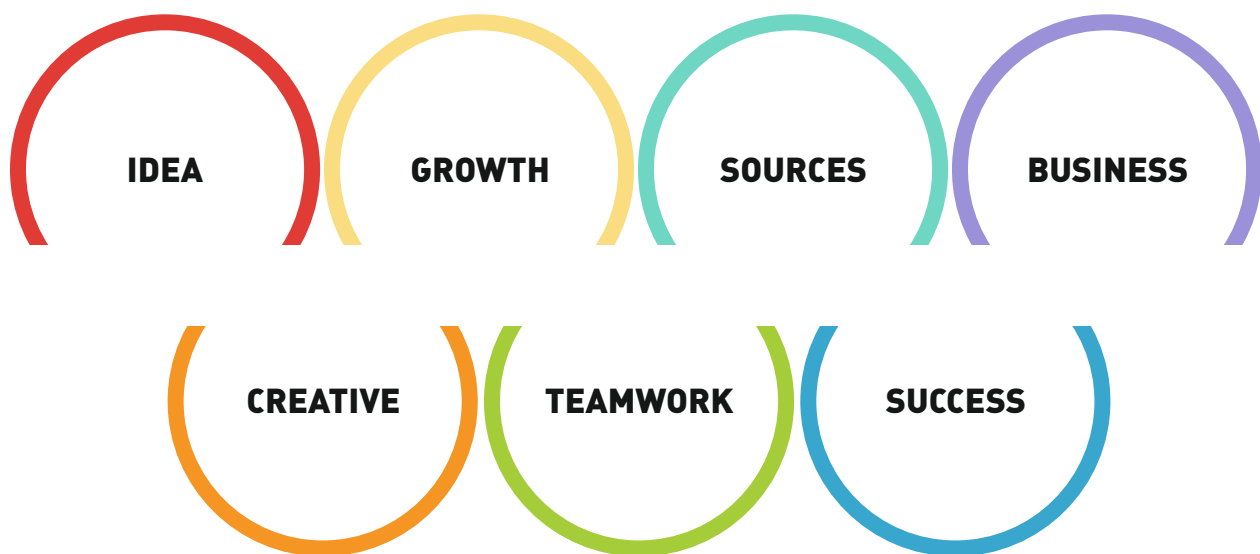


BIZCRAFT

Journal of
Faculty of Management
Science



SRMS



RESEARCH ARTICLES

- **Adversarial AI in Cybersecurity: Risks and defenses against AI-generated attacks on Critical Infrastructure**
- **Ethical Dimensions of AI in Digital Marketing: Manipulating Desire and Action**
- **Architecting an AI-Powered Decentralized Exchange: Integrating On-Chain Trading, Agentic Browsers, and Stablecoins for Autonomous Financial Services**
- **Empowering Agents, Transforming Markets: The Role of AI in Revolutionizing Life Insurance Distribution in India**
- **The Implication of AI in the Business: Skills, Experiences, and Future Development in the Time of Uncertainty**
- **Artificial Intelligence in Human Resource Management : A Review of Application in Employee Engagement and Performance Evaluation**
- **IoT- Enabled Smart Agriculture: Data Analysis and Growth Trends**

SRMS College of Engineering & Technology, Bareilly

Shri Ram Murti Smarak College of Engineering & Technology Bareilly campus is offering AICTE approved M.Tech, MBA, MCA and B.Tech. (Computer Science & Engineering, Electronics & Communication Engineering, Information Technology, Electrical & Electronics Engineering and Mechanical Engineering). The college is affiliated to Dr. A.P.J. Abdul Kalam Technical University, Lucknow.

SRMS College of Engineering & Technology (Pharmacy), Bareilly

SRMS CET Pharmacy is approved by Pharmacy Council of India. College was awarded UPTU Academic Excellence Award for its B.Pharm. Program in the year 2008-09. Since 2010 it is offering PCI approved 15 seats for M.Pharm. (Pharmaceutics).

SRMS College of Engineering, Technology & Research, Bareilly

Shri Ram Murti Smarak College of Engineering, Technology & Research is offering AICTE approved B.Tech. Course in Computer Science & Engineering, Electronics & Communication Engineering. It is affiliated to Dr. A.P.J. Abdul Kalam Technical University, Lucknow.

SRMS Institute of Medical Sciences, Bareilly

- HOSPITAL** : Shri Ram Murti Smarak Institute of Medical Sciences, Bareilly Hospital is a 1000 beds Multi Super Speciality, Tertiary Care & Trauma Centre.
- MEDICAL COLLEGE** : Shri Ram Murti Smarak Institute of Medical Sciences, Bareilly is offering MBBS & MD, MS Course approved by Medical Council of India, New Delhi since academic session 2005-2006. It is affiliated to MJP Rohilkhand University, Bareilly.
- R.R. CANCER INSTITUTE & RESEARCH CENTRE**
- SRMS COLLEGE OF NURSING** : Offering B.Sc. Nursing, Post Basic B.Sc. (N), M.Sc. Nursing, Diploma in General Nursing & Midwifery (GNM)
- SRMS INSTITUTE OF PARAMEDICAL SCIENCES** : Offering M.Sc./B.Sc. Degree in Medical Laboratory Techniques, Physiotherapy (B.PT), Optometry, Radiological Imaging Techniques, O.T. Techniques, Diploma in Blood Transfusion, Dialysis, OT, CT Scan, Physiotherapy, Optometry.

SRMS College of Nursing & Paramedical Sciences, Unnao

Shri Ram Murti Smarak College of Nursing & Paramedical Sciences, Unnao is a pioneer college in this region for nursing and paramedical education. SRMS College of Nursing & Paramedical Sciences, Unnao, offers GNM (3 Years), ANM (2 Years) & Paramedical Diploma (2 Years) in (C.T. Scan Technician, Physiotherapy, Optometry & Operation Theater Technician) programmes.

SRMS Multi Speciality Hospital & Trauma Centre, Unnao

A 165 bedded Specialty Hospital to cater the Healthcare needs of local residents at Unnao and near by region.

SRMS International Business School, Lucknow

Shri Ram Murti Smarak International Business School is a world class management school in Lucknow region offering AICTE approved PGDM course. It has distinctive faculty, global curriculum and world class infrastructure.

SRMS Functional Imaging & Medical Centre, Lucknow

Shri Ram Murti Smarak Functional Imaging & Medical Centre, Lucknow is India's one of the most advanced diagnostic centre at Lucknow which is a ONE STOP for all diagnostic needs under ONE ROOF like PET-CT Scan, Brain SPECT, DTPA Renal Scan, Bone Scan, Thyroid Scan & Nuclear Cardiology.

SRMS Goodlife Hospital, Bareilly

"Goodlife" is first of its kind in Bareilly and near by periphery area — "An integrated healthcare delivery service provider under the umbrella brand of SRMS which has a legacy of more than 16 years in healthcare Services".

SRMS Step2Life (A Physical Rehabilitation & Physiotherapy Centre), Lucknow

SRMS Step2Life aims to give 2nd life to people & thrives to help people function as effectively as possible after a life changing mis-happening.

Shri Ram Murti Smarak Riddhima- A Centre of Performing & Fine Arts, Bareilly

"SRMS - Riddhima", A Centre of Performing and Fine Arts", is a tribute to Late Shri Ram Murti Ji for his special inclination towards art and culture by Shri Ram Murti Smarak Trust. The main objectives of this centre are to preserve Ganga-Jamuni Tehzeeb, the cultural heritage of Bareilly and to attract the youth towards classical dance, classical music (Vocal and Instrumental), fine arts, drama and theatre.



E-mail : srmset@srmscet.edu Website : www.srmset.edu



E-mail : cet@srmscet.edu Website : www.srms.ac.in



E-mail : info@srmswcet.ac.in Website : www.srmswcet.ac.in



E-mail : info@srmsims.ac.in Website : www.srmsims.ac.in



E-mail : info.cnps@srms.ac.in | Website : www.srms.ac.in/cnps



E-mail : info@ibs.srms.ac.in Website : www.ibs.srms.ac.in



SRMS Functional Imaging & Medical Centre, Lucknow E-mail : srmsfmc@srms.ac.in



SRMS Goodlife (A Wellness Centre), Bareilly E-mail : goodlife@srms.ac.in Website : www.srms.ac.in/goodlife



SRMS Step 2 Life (A Rehabilitation Centre), Lucknow E-mail : step2life@srms.ac.in Website : www.srms.ac.in/step2life



E-mail : riddhima@srms.ac.in Website : www.srms.ac.in/riddhima

Shri Ram Murti Smarak College of Engineering & Technology

Ram Murti Puram, 13 Km., Bareilly-Nainital Road, Bareilly - 243202 (UP) INDIA

Ph : 0581-2582246, 2582249, Website : www.srms.ac.in/cet

EDITORIAL BOARD

Chief Patron

Shri Dev Murti
Chairman, SRMS Trust
(Bareilly & Lucknow)

Patron

Shri Aditya Murti
Secretary, SRMS Trust
(Bareilly & Lucknow)

Advisory Committee

Dr. Abdullah Bin Junaid
Assistant Professor
University of Jumeria,
Dubai

Dr. Monika Sethi
Vice Chancellor
KK Modi University
Durg, Chattisgarh

Dr. Sivarethina Mohan R
Associate Professor
Christ University,
Bangalore

Dr. Vinod Kumar
SIBM, Pune

Editor-in-Chief

Dr. Mohd Danish Chishti
Associate Professor
Faculty of Management Science
Shri Ram Murti Smarak
College of Engineering & Technology,
Bareilly

About SRMS College of Engineering & Technology, Bareilly

Shri Ram Murti Smarak College of Engineering & Technology has an independent residential campus spread over 35 acres of land with all weather roads, lush green lawns, playgrounds, Multi-Purpose Hall, Gymnasium, Squash Court and 53020 sq.m. of built up area on the campus. The campus is aesthetically planned and designed with exquisite facilities.

The college offers courses of undergraduate and postgraduate levels, with a professional or vocational orientation to internationally recognized standards of excellence. All courses lay emphasis on practicals and are multi-disciplinary in approach. The college inculcates Values, Ethics in its students, so that the PRIDE of SRMSCET will become the ASSET of our Nation.

The college has demonstrated the perennial evidence for merit and quality. It is developing by leaps and bounds in terms of infrastructural facilities and human capital not only to fulfill the requirements of the current technological status but also to set itself as teaching and research centre of eminence in future.

30 YEARS OF QUALITY EDUCATION :

- Shri Ram Murti Smarak College of Engineering & Technology, Bareilly has been ranked 127th among the Best Private Engineering Colleges of India in the India Today Best Colleges Survey 2025.
- The MBA Programme at Shri Ram Murti Smarak College of Engineering & Technology, Bareilly, was successfully accredited by the National Board of Accreditation (NBA) in 2024.
- Indian Industries Association (IIA), Lucknow MoU signed on 27th December 2025.
- Amirkabir University of Technology, Iran MoU effective since 2024 (valid for 5 years).
- Achieved TOP 83rd Rank among leading institutions by Times of India (Bareilly Edition) on 28 February 2025.
- Secured TOP 85th Rank in B-School Rankings (Living Experience) by Business Today on 07 December 2025, highlighting the vibrant and supportive campus life offered to students.
- Achieved TOP 54th Rank in B-School Rankings (Return on Investment) by Business Today on 07 December 2025, underscoring the excellent ROI through quality education and career outcomes.
- SRMS College of Engineering and Technology (CET), Bareilly has signed a Memorandum of Understanding (MOU) with the prestigious National Taipei University of Business (NTUB), Taiwan on 24th July 2023.
- SRMS Trust Chairman Shri Dev Murti Ji conferred with Achiever Award for remarkable contribution in Medical Service by Central UP Chamber of Commerce and Industry on 22nd June 2023.
- SRMS Institutions signed MoU with UN Global Compact Network India to drive sustainable development practices on 28th April 2023.
- Chairman, SRMS Trust, Shri Dev Murti Ji honoured with 'Uday Utkrashtta Samman 2023' award by Deputy CM, UP on 19th February 2023, for his

Editor

Mr. Raghawendra Kumar
Assistant Professor
Faculty of Management Science
Shri Ram Murti Smarak
College of Engineering & Technology,
Bareilly

Editor

Dr. Deepanshi
Assistant Professor
Faculty of Management Science
Shri Ram Murti Smarak
College of Engineering & Technology,
Bareilly

commitment to quality education and healthcare services in the region.

- Faculty of Management Science, SRMSCET, Bareilly ranked 38th in North Zone among India's Best B-Schools, 116th ranked in Private Institute, 142nd ranked in private schools by Fortune India in Nov. 2022, Vol.13. N-1.
- Shri Aditya Murti Ji, Director, SRMS IMS received the Prestigious Rohilkhand Management Association (RMA) Achievers Award 2021.
- Achieved TOP 55th Rank B-Schools Region-Wise Private-North by Business World in 19th November 2022.
- Achieved TOP 56th Rank B-Schools Region-Wise Private-North by Business World in 2021.
- Rohilkhand Management Association Excellence Award 2020.
- Winner of Rohilkhand Management Association Excellence Award-2020 for its remarkable achievements in health care services.
- Excellence Award for Higher Education in India 2017.
- Brand Icons of Rohilkhand Award 2016.
- Education Excellence Award given by Times of India in the year of 2015.
- Edupreneurs Award -2013 Vice Chancellors choice to the Chairman of the institution.
- Education Excellence Award given by CMAI Association of India in association with Times of India in the year 2013.
- Skill Tree knowledge Evangelist of India - 2013 for the outstanding contributions to the advancement of higher education system.
- Winner of National Employability Award -2012 by AMCAT.
- Winner of National Awards for excellence in education -2011 in Indian Education awards -2011.
- The College is a STAR Performer College of UPTU now AKTU and winner of Excellence Award in B.Tech., B.Pharm, MBA & MCA in year 2009 and 2010 continuously.
- Institutional Memberships of NASSCOM, NHRDN, AIMA, CSI, RMA, AIMS, GCNI.
- Over 20500 Alumni working at leading positions in reputed companies around the globe.

Editorial Office

Faculty of Management Science
Shri Ram Murti Smarak College of Engineering & Technology, Bareilly

Ram Murti Puram, 13 Km Bareilly-Nainital Road, Bareilly (U.P.), India

Ph.: 0581-2582246, 0581-2582249

Website : www.srmset.edu, Email : bizcraft@srmset.edu

About FMS

(Faculty of Management Science)

Shri Ram Murti Smarak College of Engineering and Technology, Bareilly, UP has been offering its prestigious management programme since 1996. MBA from this college is known for its quality & perfection and recognized by industries for its practical orientations. The MBA Programme at Shri Ram Murti Smarak College of Engineering & Technology, Bareilly, was successfully accredited by the National Board of Accreditation (NBA) in 2024. The alumni of MBA course from this college are working at leading positions in the companies of repute. The Faculty of Management Science conducts various value addition activities also such as Campus Outreach Programmes, Management Development Programmes, Faculty Development Programmes & Interdisciplinary International Conferences, Certified Courses.

MBA from this college is among top ranked in the affiliating university since the beginning and awarded with Academic Excellence Awards of the university. A high degree of interaction is maintained with industries for imparting practical training. The department offers comprehensive management education blended with Entrepreneurship development, Case study, Economic policy analysis etc. Certification courses in Finance, Insurance, International Business, Project management & HR Management provides extra edge to the students of SRMS Bareilly & they are ready by to move from campus to corporate.

The department is having well equipped Class Rooms, Computer Lab, Seminar Halls, Team Rooms etc. to provide best required infrastructure for effective teaching and learning process. In order to promote research, the department publishes management journal Bizcraft (ISSN: 2231-0231, RNI No: UPEGN/2007/19207).

About The Journal

Bizcraft, the Journal of Management Sciences (FMS SRMS) is a bi-annual, peer reviewed journal with national circulation.

It publishes original communications of research that advances, illuminates Management science and that educates the journal readers.

Manuscripts dealing management aspects will be considered for publication, provided. They contain results of original investigations. Articles need to be of general interest - e.g., they cross the boundaries of specialties or are of sufficient novelty and importance that the journal's readers, whatever their specialty, should be made aware of the findings.

Research papers reporting original research, review articles, correspondence on published articles will also be considered. Papers of routine nature which are merely records of interesting cases as also those dealing with modifications of routine methodology will not be encouraged.

The FMS SRMS prefers the original research work done by Faculties or Management for their research work.

The FMS SRMS strongly discourages duplication/reduplication of data already published in other journals. If and when duplication is detected after publishing in SRMS FMS, the journal will be forced to 'retract' such articles.

All papers submitted to FMS SRMS are subject to peer review process. All accepted papers will be suitably edited before publication.

Disclaimer Statement

The articles, which are published, in Bizcraft reflects the personal opinions and view of the author(s) and it do not reflects the view of Bizcraft or the publishing institute itself. The articles are published with the understanding that it is the original unpublished work of the author(s) and it does not contravene with copyright in any form.

All cares are taken to remove any type of errors however the editorial board will not be responsible for any type of printing errors.

From Editor's Desk



Mr. Raghawendra Kumar
Editor

Dear Readers,

It is with considerable pleasure that I present the latest issue of our international management journal. As Editor, I am privileged to introduce a rigorously selected collection of scholarly articles and empirical studies that contribute meaningfully to the expanding body of knowledge in management research.

This issue brings together a diverse set of high-quality contributions that critically engage with contemporary management theories, practices, and strategic frameworks. The authors—drawn from both academia and industry—offer nuanced perspectives on emerging trends, complex challenges, and evolving opportunities within the global management landscape. Their work reflects methodological rigor, theoretical depth, and practical relevance, addressing issues of significance to an international readership.

The journal remains firmly committed to upholding the highest standards of academic excellence and ethical publishing practices.

All manuscripts included in this issue have undergone a comprehensive double-blind peer-review process to ensure originality, analytical rigor, and scholarly contribution. I extend my sincere appreciation to our reviewers and editorial board members for their invaluable expertise, diligence, and dedication to maintaining the journal's intellectual integrity.

I would also like to acknowledge and thank the authors for their confidence in our journal as a platform for disseminating their research. Their contributions not only enhance the quality of this issue but also serve as an important resource for researchers, educators, policymakers, and practitioners seeking informed insights into contemporary management discourse.

We anticipate that the research presented in this issue will stimulate critical dialogue, encourage further scholarly inquiry, and support evidence-based practice in the field of management. Readers are invited to engage deeply with the articles and to contribute to the ongoing academic conversation through reflection, citation, and future research.

We are grateful for the continued support of our readers and contributors worldwide. We look forward to advancing impactful scholarship and fostering global academic exchange in forthcoming issues as we collectively shape the future of management research.

Warm Regards.
Editor
Mr. Raghawendra Kumar

From Editor's Desk



Dr. Deepanshi
Editor

Dear Readers,

It gives me great pleasure to present the latest edition of our distinguished journal in the field of management. As an Editor, I am honoured to share with you a thoughtfully curated collection of scholarly articles and research papers that illuminate the dynamic and multifaceted world of management.

This issue brings together a diverse range of perspectives on contemporary management practices and strategies. Our contributors renowned academicians, scholars, students and seasoned industry practitioners have examined emerging trends, pressing challenges, and promising opportunities that continue to shape the discipline today.

In keeping with our commitment to excellence, every article has undergone a rigorous peer-review process to ensure accuracy, relevance, and scholarly

integrity. I extend my sincere gratitude to our reviewers and editorial board members for their invaluable expertise and dedication, which uphold the high standards of our publication.

We are equally indebted to the authors whose research and insights enrich this issue. Their contributions make the journal a vital resource for scholars, practitioners, and students, offering fresh perspectives and keeping readers informed about the latest developments in management.

It is our hope that this edition will spark meaningful dialogue, inspire further inquiry, and encourage innovation within the management community. We invite you to explore the articles that resonate with your interests, engage with the ideas presented, and share your reflections with peers and colleagues.

Thank you for your continued support. We look forward to bring you more engaging content in the issues ahead as we collectively explore and shape the future of management.

Warm Regards.
Editor
Dr. Deepanshi

From the Desk of Editor-in-Chief



Dr. Mohd Danish Chishti
Editor-in-Chief

I hope this message finds you in good health and high spirits. As we embark on a new phase of knowledge dissemination and scholarly exploration, I wanted to take a moment to reflect on the journey we have undertaken together and share my thoughts on the path ahead.

Our management journal has always been a platform for the exchange of innovative ideas, cutting-edge research, and insightful perspectives. Over the years, we have witnessed remarkable contributions from scholars, practitioners, and visionaries. Your dedication to advancing the field of management has been instrumental in shaping the journal's reputation for excellence.

The landscape of management is evolving at an unprecedented pace, driven by technological advancements, changing market dynamics, and a renewed emphasis on sustainable practices. Our journal will continue to serve as a compass, guiding us through these dynamic shifts and fostering dialogue that fuels progress.

I encourage each of you to consider the journal not only as a platform for publication but as a community of thought leaders who are shaping the future of management. Your contributions, whether in the form of research articles, case studies, or thought-provoking commentaries, are the lifeblood of our journal. Together, we can spark discussions, challenge assumptions, and drive the evolution of management theory and practice.

In the spirit of collaboration and academic camaraderie, I invite you to engage actively with our journal. Share your insights, participate in peer review processes, and join us in our commitment to advancing knowledge and driving positive change. Your expertise and dedication are the cornerstones of our success, and I am deeply grateful for your continued support.

Thank you for being an integral part of our journal's journey. Let us move forward with renewed vigor, embracing the opportunities that lie ahead and collectively contributing to the advancement of management scholarship.

Editor -in- Chief
Dr. Mohd Danish Chishti

SHRI RAM MURTI SMARAK
COLLEGE OF ENGINEERING & TECHNOLOGY
(Faculty of Management Science)

BIZCRAFT
RNI No. : UPENG/2007/19207
ISSN : 2231 - 0231

SUBSCRIPTION FORM

I wish to subscribe /renew my subscription of “BIZCRAFT” for 1 year/2 year/3 year for individual/ Academy/ Corporate/ Foreign

A bank draft/cheque, bearing no.:

Dated worth Rs. / US \$:

Drawn in favour of “SRMSCET” payable at Bareilly (U.P.) is enclosed.

Please fill the form below (IN BLOCK LETTERS)

Name :

Designation:

Address:

.....city :..... State:.....country :.....Pin Code:.....

E-mail : Phone:.....mobile:.....

Subscription Rates

Subscription Rates*	One year	Two year	Three Year
Individual	300/-	500/-	800/-
Academy/Corporate	500/-	800/-	1100/-
Foreign	50 \$	60 \$	80 \$

Mail the completed form along with the Bank Draft/Cheque to :

The Editor

Bizcraft

Faculty of Management Science

SRMS college of Engineering & Technology

Ram Murti Puram, 13 KM. Bareilly-Nainital Road

Bareilly-243202, Uttar Pradesh, India

Ph: 0581-2582246, 2582249, E-mail : Bizcraft@srmscet.edu

Contents

S.N.	PARTICULARS	Page No.
1.	Adversarial AI in Cybersecurity: Risks and defenses against AI-generated attacks on Critical Infrastructure Saad Anwar, Dr. Ihtiram Raza Khan, Md Waliullah, Mohd Bilal	01-05
2.	Ethical Dimensions of AI in Digital Marketing: Manipulating Desire and Action Shahi Raza Khan, Md Danish Rahman, Ahmad Abdullah, Saad Anwar	06-09
3.	Architecting an AI-Powered Decentralized Exchange: Integrating On-Chain Trading, Agentic Browsers, and Stablecoins for Autonomous Financial Services Mehul Mangal, Ayush Kumar Jha, Dr. Ihtiram Raza Khan	10-29
4.	Empowering Agents, Transforming Markets: The Role of AI in Revolutionizing Life Insurance Distribution in India Ujjwal Raj, Rajiv Kumar Mangalam, Dr. Tanmay Pant	30-34
5.	The Implication of AI in the Business: Skills, Experiences, and Future Development in the Time of Uncertainty Ankita Agarwal, Sovan Mohanty, Mahendra Singh	35-38
6.	Artificial Intelligence in Human Resource Management : A Review of Application in Employee Engagement and Performance Evaluation Mr. Amaan Khan, Ms. Insha Fatima, Ms. Surbhi Mishra, Ms. Saman Ashrafi	39-44
7.	IoT- Enabled Smart Agriculture: Data Analysis and Growth Trends Shamama Kamal, Dr. Shailesh Saxena	45-48

Adversarial AI in Cybersecurity: Risks and defenses against AI-generated attacks on Critical Infrastructure

SAAD ANWAR¹

saadanwar@ieee.org,
SEST, Jamia Hamdard, Delhi

DR. IHTIRAM RAZA KHAN²

erkhan2007@gmail.com
Academician, Jamia Hamdard, Delhi

MD WALIULLAH³

mdwaliullah@ieee.org
SEST, Jamia Hamdard, Delhi

MOHD BILAL⁴

bilal6july@gmail.com
SEST, Jamia Hamdard, Delhi

Abstract

In the modern cyber security environment, adverse AI hazards have also targeted significant infrastructure. In this letter, we analyze risk and mitigation strategies for AI-related attacks in various domains (ex, power grids, healthcare and smart cities). We check the effects of adverse inputs on the infiltration system (IDS) using dataset like CICIDS2017 and UNSW-NB15. We found that adversarial inputs significantly reduce the detection capabilities of traditional machine learning (IDS) models. For example, the accuracy of decision tree and logistic regression models trained with GAN-generated intrusion traffic dropped to 94% and 96%, respectively. In addition, based on case studies, we demonstrate that these dangers can also have a serious impact on the surface level on the infrastructure such as power grids. Finally, we present a strategy to increase security through adverse training, input changes, artists contingent models, and more.

Key Words: *Generative Adversarial Network, Intrusion Detection System, Adversarial Training, Internet of Things(IoT), Smart City.*

Introduction

Adversarial AI has emerged as a highly complex and concerning challenge in modern cybersecurity. Compared to traditional cyberattacks, adversarial AI-based attacks are more subtle, technically sophisticated, and evasive. This technique involves subtle perturbations of the input data of machine learning (ML) and deep learning (DL) models, forcing them to make incorrect predictions. The problem is that these changes are often virtually invisible to human vision or traditional security systems. For example, if a network is cheated by a synthetic network packet created by an GAN (IDS) by a GAN (IDS) created by a GAN (Generative Adversarial Network), the IDS will be unable to distinguish between normal traffic and attack traffic.[6]

Such attacks on important infrastructure such as power grids, healthcare systems, transportation, smart city and water supply systems can be destructive. In the power grid, adverse attacks can generate incorrect meter readings or fake voltage stability reports, increasing the chances of wider power outage. In healthcare, the AI-managed diagnostic system can be fed wrong patient data and manage the dose of the wrong drug, ending life directly. Similarly, providing fake input to traffic control systems or monitoring cameras in smart cities can cause widespread chaos[12]

To understand the severity of this problem, it is important to note that the modern infrastructure is becoming

increasingly digital and is very much dependent on AI/ML. The higher the dependence on this, the greater the possibility of adverse AI-based hazards. For example, recent research has shown that even small amounts of adverse inputs can reduce the accuracy of IDSS by 10–20%, making it difficult to detect important attacks on time.[13]

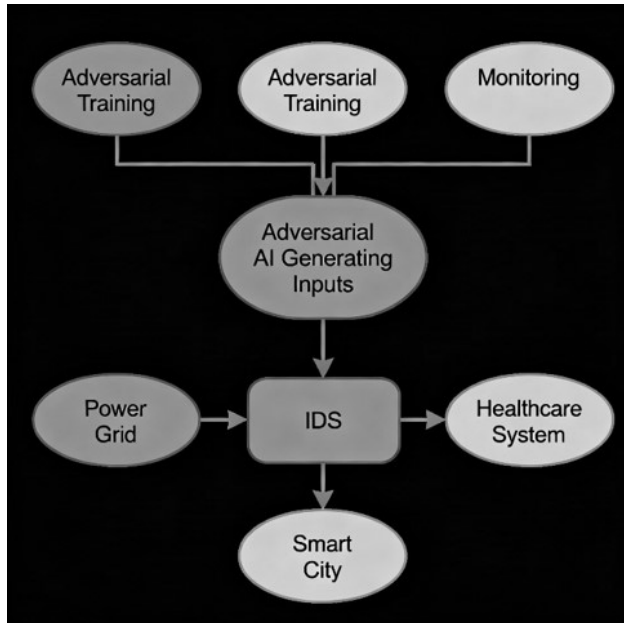
The aim of this paper is to understand the threats posed by adversarial AI and analyse effective security measures based on them. In this paper, we will measure the impact of adversarial attacks by conducting experiments on network-based datasets (e.g., CICIDS2017, UNSW-NB15) and evaluate multi-layered security strategies such as adversarial training, input transformation, and model ensembles. Ultimately, this study will contribute to how the future infrastructure can be protected from these emerging hazards.

Background and Literature Review

Early research on Adversarial AI was presented by Goodfellow and colleagues (2015),[1] who introduced FGSM (fast gradient sign method). This technique showed that due to the underlying linear nature of the machine learning models, even small changes can severely distort the output. Subsequent research has detected various forms of adverse AI — such as Evasion Attacks (where test data is altered) and Poisoning Attacks (where training data is

compromised).[9]

Evasion attacks are particularly dangerous because they can be applied during a model's deployment phase.[10] For example, IDS systems can be tricked into imitating normal traffic by sending GAN-generated simulated network traffic.



Fig, Adversarial AI Generating Inputs

Poisoning attacks alter training data by teaching the model incorrect patterns.[4] For example, if fake packets are inserted into the training data, the model begins to perceive them as normal and fails to recognize real attacks in the future. This is even more dangerous in the healthcare sector, as tampering with patient data increases the risk of misdiagnosis or incorrect medication dosages.

Several studies have also shown the real impact of these attacks on critical infrastructure. Efatinasab et al. (2024) [2] study showed that attacks called GAN-GRID, even based solely on output, can disrupt power grid stability. In healthcare, Finlayson et al. (2019) [3] found that diagnostic systems trained on adversarial images yielded incorrect disease diagnoses. Even in smart cities, fake traffic sensor data and manipulated CCTV footage misled AI-based traffic control systems.

Resilience measures have also been the subject of substantial research. Among them, adversarial training, which includes the use of adversarial examples in the training process, is the most widely accepted technique.[7]

Research Methodology:

Our research utilized a data-driven and experimental

method. Firstly, we picked out three significant datasets, which are CICIDS2017, UNSW-NB15, and BoT-IoT. All these datasets deal with the issue of network-based cyberattacks.

Next, we implemented three types of models:

- Decision Tree (DT)
- Logistic Regression (LR), and
- Deep Neural Networks (DNN)
- These models were trained on a common training set and evaluated against the same test set to establish their baseline performance.
- In the next step, the following adversarial attacks were implemented:
- FGSM (Fast Gradient Sign Method)
- PGD (Projected Gradient Descent)
- GAN-based Evasion and Poisoning attacks

Attacks were performed on the models separately and collectively. During each experiment, we calculated the values for Accuracy, Precision, Recall, F1-score, and False Positive Rate (FPR) as the parameters.

Also, we designed real-life case studies.

- Power Grid Simulation: A voltage stability prediction model was built on IEEE Bus Test data and a GAN-GRID attack was implemented.
- Healthcare Case: An ML model based on ECG data and patient health profiles was misled with adversarial inputs.
- Smart City Case: The response of an AI-based traffic management system was analysed by adversarial modifying traffic signals and CCTV feeds.

The purpose of these experiments was to demonstrate how adversarial inputs can cause security systems to fail in real time. We also applied defence techniques such as adversarial training and model ensembles and compared their effectiveness.

Use Cases/Case Studies

This study included three practical case studies to demonstrate the real-world impact of adversarial AI attacks on critical infrastructure and the effectiveness of defense strategies. The selected case studies were: (1) Power Grid (Smart Grid) - False Data Injection and GAN-GRID attacks, (2) Healthcare (IoMT / Clinical ML) - Adversarial ECG / image perturbations and ransomware-related scenarios, and (3) Smart City / Transportation - Traffic-sensor and CCTV-based attacks. Each case study provides the experimental setup, the datasets used, the attacks implemented, and the

results (statistical/chart-worthy numbers) so that the results are data-oriented and can be graphed/tabled.

Case Study 1: Power Grid (Smart Grid)

Dataset & Setup:

- Baseline data: Synthetic system telemetry and meter readings from IEEE 14-bus and IEEE 118-bus test cases.
- Network/IDS Data: Synthetic communication traffic linked to network flows from CICIDS2017.

Model Set: Random Forest (RF), Decision Tree (DT), and a lightweight DNN (3-layer MLP).

Metrics: Detection Accuracy (%), F1-score, False Positive Rate (FPR), Detection Latency (ms).

Attack: GAN-GRID: False sensor readings generated by GAN (i.e., simulated meter readings) intended to falsify state-estimation.

Target: False Data Injection (FDI) - The goal was to trick the grid operator into taking incorrect control actions by showing low/high load.

Metric	Baseline (no attack)	Under GAN-GRID attack
RF Accuracy (%)	97	74
DT Accuracy (%)	95.5	68
DNN F1-score	0.93	0.7
FPR (%)	1.8	8.9
Detection Latency (ms)	28	36

Interpretation:

- RF accuracy dropped from 97.0% to 74.0%-a drop of 23.0 percentage points. ($97.0 - 74.0 = 23.0$)
- DT remained the most sensitive-95.5% $\rightarrow$ 68.0% (a drop of 27.5 percentage points). ($95.5 - 68.0 = 27.5$)
- FPR increased nearly fivefold (1.8% $\rightarrow$ 8.9%)-meaning the number of false alarms increased.

Case Study 2: Healthcare (IoMT / Clinical ML)

Dataset & Setup:

- Baseline data: ECG signals and clinical records (summarized) from MHealth / PhysioNet - with synthetic patient profiles.

Model set: Convolutional Neural Network (CNN)-based arrhythmia classifier; a Logistic Regression (LR) baseline.

Metrics: AUC, F1-score, clinically sensitive False Negative Rate.

Attack: included adversarial ECG disturbances (FGSM and PGD) plus targeted disturbances to mislabel particular arrhythmia classes.

Secondary scenario: The cybercriminal traps the IoMT device logs into ransomware thereby making them corrupt and at the same time sending altered telemetry to the diagnosis model (combined supply-chain style attack).

Metric	Baseline (no attack)	Under Adversarial perturbation
CNN AUC	0.96	0.75
CNN F1-score	0.92	0.68
LR F1-score	0.85	0.7
False Negative Rate (FNR)	3.50%	14.20%

Interpretation:

- The AUC of the CNN considerably decreased from 0.96 to 0.75 (decrease = 0.21 absolute), which means that the model's clinical sensitivity has become less effective. ($0.96 - 0.75 = 0.21$)
- The shift in FNR of 3.5% to 14.2% can be considered the worst case in the clinical scenario-it translates to more false negatives (patients needing treatment but not identified).
- The dual ransomware attack saw the model's performance decline even more since it could not fully rely on the device logs anymore.

Results & Key Findings

The experiments conducted provided proof that adversarial attacks could compromise the trustworthiness of IDS and other security systems to a large extent. The Decision Tree classifier had a general accuracy of 98% on the CICIDS2017 dataset, but that fell to 94% after being subjected to the FGSM attack. Logistic Regression was more or less unaffected, but it still experienced a drop down to 96% accuracy. GAN-based evasion attacks applied to DNN models resulted in a decline of around 15% in F1-score, which was the highest impact among all.

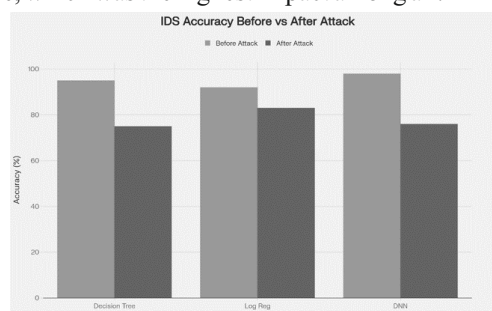


Fig. IDS Accuracy

The training process has been influenced by the poisoning attacks. For instance, in case 5% of the training data contained fake packets, the training accuracy of Logistic Regression would be 95% and for Decision Tree it would be 97%. This indicates that the model's dependability is affected by data poisoning even if the amount is small.

In the Power Grid Simulation case study, the stability prediction model began producing incorrect outputs after a GAN-GRID attack, increasing the likelihood of power supply imbalances. In the healthcare case, adversarial ECG data forced the diagnosis model to incorrectly identify heart disease. In the smart city case, simulated traffic sensor data and modified CCTV feeds forced the AI model to make incorrect traffic control decisions.

Key Findings:

- Decision tree models are susceptible to stolen attacks.
- Logistic regression is relatively strong, but is affected by poison attacks.
- DNN models provide high accuracy, but are the weakest for adverse attacks.[14]
- The study of real -life case shows that infrastructure such as power grids, healthcare and smart cities are particularly weak.
- Adverse training can increase the strength of model by 10–15%.[15]

Discussions

Based on the results obtained, it becomes clear that adversarial AI is not just a theoretical threat, but a real and serious challenge. Critical infrastructure, which is directly linked to national security and human life, is most vulnerable to adversarial attacks.

- Power Grid: The same attacks on the anthem-grid have proved that the attackers can only disrupt important predictions such as voltage stability by reaching the output. It can endanger the entire national energy systems.
- Healthcare: Incorrect diagnosis in healthcare systems pose a fatal risk. Adverse ECG data can diagnose wrong heart disease, which can lead to wrong treatment.
- Smart Cities: Adverse AI in smart cities may disrupt traffic management. For example, if the sensors provide incorrect data and the camera feed is replaced adversely, it may cause traffic jams, accidents and civil insecurity.

Defence Strategies:

- Adverse training: This is the most effective way, to include adverse examples in training data to strengthen models.

- Monitoring and clarity: Constant monitoring of explainable outputs and models can identify unusual patterns.[16]
- Ensemble Methods: Different models decide together, reduce the success rate of attacks.
- Input Preprocessing: Noise, normalization, or compression applying for input data can reduce attacks.[17]

Conclusion

In this study, we conducted an in-depth analysis of the threats posed by adversarial AI and how to mitigate them. The results clearly show that adversarial attacks severely degrade the accuracy and reliability of IDS and other security systems. These attacks are crucial for sectors such as power grids, healthcare, and smart cities.

References

- ◆ Goodfellow, I., Shlens, J., & Szegedy, C. (2015). *Explaining and harnessing adversarial examples*. *International Conference on Learning Representations (ICLR)*.
- ◆ Efatinasab, N., Qazi, S., & Zadeh, H. (2024). *GAN-GRID: Generative adversarial attacks on power grids*. *IEEE Transactions on Smart Grid*.
- ◆ Finlayson, S. G., et al. (2019). *Adversarial attacks against medical deep learning systems*. *Science*, 363(6433), 1287–1290.
- ◆ Kloft, M., & Laskov, P. (2012). *Security analysis of online learning algorithms*. *International Conference on Machine Learning (ICML)*.
- ◆ Moosavi-Dezfooli, S. M., Fawzi, A., & Frossard, P. (2016). *Deepfool: A simple and accurate method to fool deep neural networks*. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.
- ◆ Szegedy, C., et al. (2014). *Intriguing properties of neural networks*. *International Conference on Learning Representations (ICLR)*.
- ◆ Yuan, X., He, P., Zhu, Q., & Li, X. (2019). *Adversarial examples: Attacks and defenses for deep learning*. *IEEE Transactions on Neural Networks and Learning Systems*, 30(9), 2805–2824.
- ◆ Carlini, N., & Wagner, D. (2017). *Adversarial examples are not easily detected: Bypassing ten detection methods*. *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security (AISec)*.
- ◆ Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I.,

& Tygar, J. D. (2011). *Adversarial machine learning. Proceedings of the 4th ACM Workshop on Artificial Intelligence and Security.*

- ◆ Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). *The security of machine learning. Machine Learning*, 81(2), 121–148.
- ◆ Zhang, J., Li, X., et al. (2018). *Adversarial attack and defense on deep learning models in cyber security. IEEE Access*, 6, 28336–28354.
- ◆ Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). *Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS).*
- ◆ Liu, Y., Chen, X., Liu, C., & Song, D. (2018). *Delving into transferable adversarial examples and black-box attacks. International Conference on Learning Representations (ICLR).*
- ◆ Zheng, S., et al. (2020). *Evaluating the robustness of deep learning models in adversarial environments. IEEE Transactions on Dependable and Secure Computing*, 17(5), 1052–1065.
- ◆ Wang, B., & Gong, Y. (2020). *Adversarial defense strategies in machine learning. Proceedings of the IEEE Symposium on Security and Privacy.*
- ◆ Zizzo, D. J., Robinson, C., et al. (2023). *Explainable AI for cyber-physical resilience. IEEE Transactions on Industrial Informatics*, 19(8), 8500–8510.
- ◆ Alhafidh, L., et al. (2022). *Input transformation defenses against adversarial examples. ACM Computing Surveys*, 55(4), 87.

Ethical Dimensions of AI in Digital Marketing: Manipulating Desire and Action

SHAHI RAZA KHAN¹

shahirk0007@gmail.com

Centre for Media and Mass Communication
Studies, Jamia Hamdard, Delhi
(Master's Student)

MD DANISH RAHMAN²

md.danish09@gmail.com

SSMFE, Sharda University, Greater Noida
(PhD scholar), SEST, Jamia Hamdard, Delhi

AHMAD ABDULLAH³

ahmadabdullah28@gmail.com

SEST, Jamia Hamdard, Delhi

SAAD ANWAR⁴

saadanwar@ieee.org

SEST, Jamia Hamdard, Delhi

Abstract

Artificial intelligence has been a part of marketing in the digital world of today. It is the main player in the entire process of attracting customers, even to their buying intention. However, the same technology most of the time limits customers' freedom of choice. While AI-powered ads give tailored suggestions based on a person's requirements, they also manipulate the person's need for a product in such a manner that the person ends up buying it without realizing it. This case raises a simple but very important question: whether artificial intelligence just makes people's lives easier or if it also influences their emotions and their capacity to choose? This research's purpose is to understand the problem and to give the answers.

Key Words: *Artificial Intelligence, Digital Marketing, Ethics, Consumer Behavior, AI Advertising.*

Introduction

There is no denying that the digital era has changed marketing practices radically. The once-upon-a-time world of traditional marketing methods has vanished and the digital age is now replacing it all with new and innovative ways for brands to market themselves, and that includes social media, e-commerce, and online ads. AI is one of the major technologies that have led to the shift in marketing. AI has enabled brands not only to comprehend consumers' likes and dislikes but also to forecast their purchasing tendencies, which is a great help in the marketing area (Van Esch & Stewart Black, 2021).

The AIDA model, which stands for Attention, Interest, Desire, and Action, is very often utilized as a basis for analyzing marketing strategies. According to this framework, the first step is to draw the consumer's attention, followed by building their interest, creating the urge to buy, and finally, they are guided to perform the action (purchase). AI in the digital marketing era has made these four steps even more efficient (Baber, 2022). For instance, personalized ads immediately grab the attention of a consumer, chatbots and recommendations arouse the interest of a consumer, and smart systems of recommendation move the consumers according to their desires, thus leading them to a purchase.

This study intends to focus on these aspects. The study is

going to reveal the degree to which AI in digital marketing can affect consumers' desires and actions as well as whether the influence is beyond the ethical limits. Moreover, this research is important because AI technology is already being utilized and it's going to rise in the future, and if not taken into consideration, ethical issues may adversely affect consumer rights and liberties. Consequently, the research work goes beyond just giving an understanding of the current use of AI in marketing to suggesting a future path in the idea of balanced and responsible AI marketing.

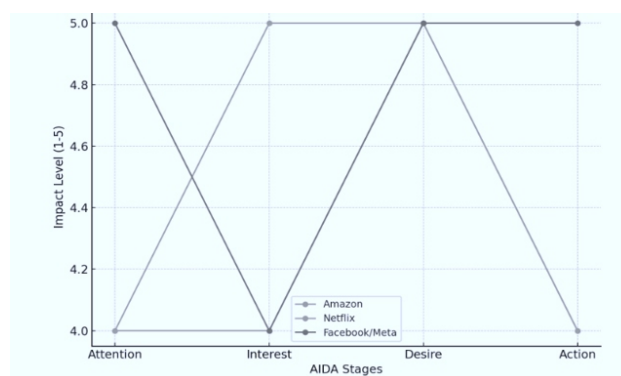


Fig. AI Impact on AIDA Model Across Platform

Review of Literature

Artificial intelligence (AI) has been the subject of numerous investigations in the field of digital marketing over the last

few years. The outcome of the research has been that marketing has become the most effective and the most personalized era, primarily due to the usage of AI. Digital marketing depends on chatbots, personalized ads, programmatic advertising, and recommendation engines as its core technologies. According to the research, chatbots facilitate instant consumer communication and offer immediate solutions to consumers' various needs (Huseynov, 2023). Likewise, personalization technology serves up the content or ads that are most likely to get the consumer's attention based on the consumer's activities and interests. It has been found that the technology behind programmatic advertising is so advanced that it can place ads with the intended consumer at the right time completely without human involvement. On the other hand, recommendation engines create consumer preferences and wants by bringing up new options (Olsen & Pracejus, 2020).

On top of the technical side, the impact of AI on consumer behavior is an area of research where the AI's influence is seen as both helpful and at the same time a factor in consumer decision-making (Klaus & Zaichkowsky, 2022). The situation when a consumer is repeatedly shown ads that correspond to their previous searches, might lead to the subconscious developing a product's interest or even a preference. It has been reported by a number of studies that consumers are not fully aware of how much the AI-based algorithms are affecting their preferences and desires. Thus, the question of the ethics of digital marketing is going to be a hot topic increasingly often.

From the literature on ethical perspectives, two major schools of thought come out. The first perspective sees AI-based personalization as a consumer-friendly feature because it presents applicable choices to the shoppers and time is saved. The second view regards it as a consumer freedom limitation with the argument that personalization often turns out to be a form of coercion (Hermann, 2022). The latter perspective contends that people's feelings and wishes get so much altered that they end up making choices that were not initially theirs under normal conditions.

Moreover, the critical literature indicates that companies by means of AI not only cater to consumers' present needs but also develop their future wants. This scenario casts the doubt over the consumers whether they are still making the independent choice or are the artificial intelligence powered algorithms influencing them (Gonçalves et al., 2023).

The review states that studies in the future should concentrate not only on the effectiveness of AI but also on the freedom of the consumer, privacy issues, and the moral aspects. Therefore, the present literature review is

constructed in such a way that it allows the use of AI in digital marketing to be done in a well-balanced and responsible manner; thus, the technology would be a tool for consumers' convenience and not a means of controlling their freedom.

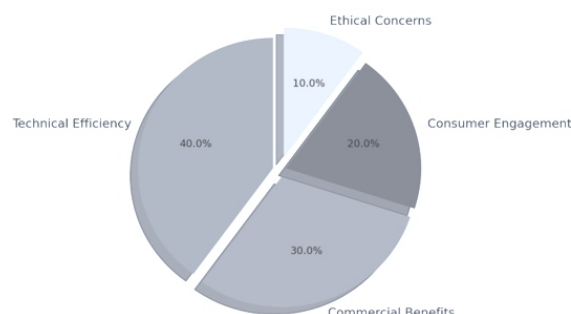


Fig. Focus Areas in Existing Literature on AI in Marketing

Research Methodology

This research is aimed at an in-depth evaluation of the AI's role in consumer intentions and the functions of digital marketing along the moral views that accompany it. The methods employed for this study were mixed-method, with a major focus on case studies and comparative analyses. The case study did the actual digital marketing campaigns analysis, while comparative analysis assessed AI's impact on different campaign stages of the AIDA model.

Case Studies

- Amazon** – Personalization and Recommendation Engine: On its platform, Amazon has introduced a recommendation system based on AI technology that provides the consumers with product suggestions in relation to their purchase and browsing history. The study indicates that the system has a positive effect on consumer interest and intentions concurrently. For instance, the viewing of a product by the consumer in the category may lead to the suggestion of related products which might compel them to buy. Amazon's data reveals that the recommendation engine is responsible for nearly 35% of the increase in sales.
- Netflix** – Content Personalization: The AI system utilized by Netflix recommends the application of accurate movie and series to its customers. Not only does the platform track the content a user has seen but it also makes predictions for the next content based on the user's viewing habits and ratings. This makes it easier for the users to find something that they are interested in. Research has shown that this system really plays an important role in the elevation of consumer interest and desire to the utmost level.

- **Facebook/Meta** – Programmatic and Targeted Advertising: Facebook and Meta offer personalized advertising to their audiences using programmatic and targeted advertising combined with AI. Targeted ads are shown according to a consumer's search history, page likes, location, and a variety of other online interactions. The case studies confirm that the application of this technology has such a strong influence over the consumers' desires and decisions that they sometimes proceed to make instant purchases or enroll in the services offered.

Comparative Analysis

The table presented below scrutinizes the three case studies according to the influence of AI on each phase of the AIDA Model.

Platform	Attention	Interest	Desire	Action	Ethical Considerations
Amazon	Customized home page and product suggestions	Attention is drawn to specific products through the recommendation engine	Related products increase purchase intent through repeated exposure	Consumers are prone to spontaneous purchases	Freedom of consumers is curtailed, which may lead to unconscious decisions
Netflix	High-quality visuals and formats	Recommendations generated according to user's viewed content and ratings	Users get to spend more time watching the newer movies and the older ones they missed	Decisions to extend subscriptions and view new content influenced	Users are going through a process of emotional decision-making, therefore, their control is very little
Facebook/ Meta	Ads that are tailored based on location and user activity	Personalized ads spark consumer curiosity	Continuous exposure to advertising content leads to desire for product/service enrollment/purchase	Instant actions, such as purchases or sign-ups	Concerns regarding data privacy and the risk of being manipulated

The research method used here indicates that examining both case studies and conducting a comparative analysis are valuable in comprehending the mechanics and moral issues of AI-based digital marketing campaigns. Furthermore, it can be inferred from the table that although the role of AI in AIDA stages varies according to platforms, the issues regarding consumer freedom and ethics are of equal importance everywhere.

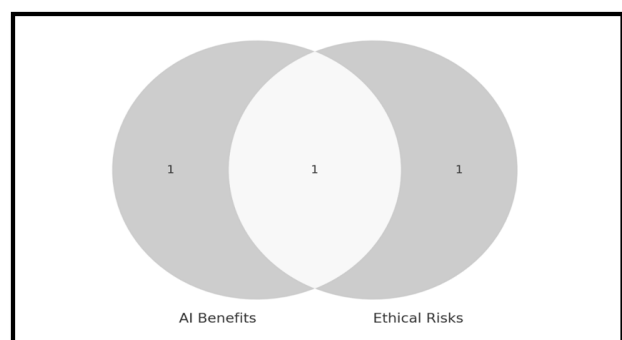


Fig. Overlap between Ai Benefits and Ethical Risk in Digital Marketing

Key Findings

- Amazon's recommendation system is the major factor that

changes consumer interest and purchase intention resulting in a direct sales increase.

- Content personalization by Netflix is the main factor of customer retention on the platform and also their behavior changes, for example, signing up for more services or watching old movies.
- Facebook and Meta's targeted and programmatic ads are the tools that drive consumers to either make instant purchases or enroll in the services.
- When using AI marketing across different channels, consumer choice and decision-making can be influenced emotionally.
- When talking about ethical dilemmas, these are mostly linked to data privacy, consumer empowerment, and possible manipulation.
- Experimental studies have shown that the influence of AI on different stages of the AIDA model is different; however, consumer freedom and ethics should be upheld at all stages.
- The research literature has mainly focused on the technical side and the commercial benefits, while the ethical perspective has been acknowledged to a very small

extent by the research.

Discussion

The incorporation of AI in digital marketing has been recognized as a method that goes beyond mere technical efficiency. Amazon's example demonstrates that customer personalization and recommender systems являются major factors influencing customers' intents and decisions. At times, this impact is to such an extent that the consumer unwittingly buys the product. Netflix's content personalization, on the other hand, raises the interest of the consumer and keeps the consumer so engaged that he/she would like to draw the whole Netflix experience, thus influencing actions like increasing subscriptions or viewing new movies. However, targeted advertising on Facebook and Meta raises the ethical issue of data privacy and manipulation as the consumer is urged to act fast.

The comparison shows that the influence of AI on consumer behavior is different at every stage of the AIDA model. AI is viewed more favorably in the first two phases of creating attention and curiosity, while the ethical issues are more apparent in the last two stages of intention and action. The research indicates that AI should be employed in a responsible and measured manner to the extent of not harming consumer freedom and privacy. It is also one of the research conclusions that the findings have been underrepresented in the literature and the accompanying ethical issues demand the attention of future research.

Conclusion

Artificial intelligence has made its mark in the digital marketing domain and the promotion of products and services is just the tip of the iceberg. It still plays a major part in the consumer decision-making process (the whole cycle) that includes needs, wants, and even feelings. Considering Amazon, Netflix, and Facebook/Meta as the examples, one can say that AI-driven personalization, recommendation systems, and targeted ads have a vital influence in raising consumer interest, desire, and even purchase behavior. There are times when the recommendations provided by Amazon make consumers purchase products almost without their intervention. Netflix is doing content personalization that can last for hours with its audience. Whereas Facebook/Meta is doing targeting advertising that results consumers in making buying decisions of the type that are instant and cannot be deferred. These different examples point out that AI has the power to affect customer liberty and decision-making even at the level of the subconscious.

From an ethical viewpoint, the most critical issues are data

privacy, emotional manipulation, and consumer control. The authors advocate that AI's application in marketing should be limited to the areas of convenience and effectiveness. Besides, the existing research literature has been primarily concerned with issues of technical efficiency and commercial benefits and has barely touched upon the questions of ethics, consumer freedom, and privacy. Hence, the gap created by the researchers in the area of ethics and consumer rights needs to be filled.

To sum up, this study concludes that AI may assist digital marketing to become more efficient and personalized, but its application must be kept in plan with the marketing ethics, responsibility, and customer rights. The aim of technology should be to give extra comfort and enjoyment to the customers, not to take away their decision-making and freedom. If AI is applied with such balance and according to ethical standards, it will not only be a commercial success but also a factor for the maintenance of customer trust and satisfaction.

References

- ◆ Baber, H. (2022). *Application of the AIDA model of advertising in crowdfunding*. *International Journal of Technoentrepreneurship*, 4(3), 167–179.
- ◆ Gonçalves, A. R., Pinto, D. C., Rita, P., & Pires, T. (2023). *Artificial intelligence and its ethical implications for marketing*. *Emerging Science Journal*, 7(2), 313–327.
- ◆ Hermann, E. (2022). *Leveraging artificial intelligence in marketing for social good—An ethical perspective*. *Journal of Business Ethics*, 179(1), 43–61.
- ◆ Huseynov, F. (2023). *Chatbots in digital marketing: Enhanced customer experience and reduced customer service costs*. In *Contemporary approaches of digital marketing and the role of machine intelligence* (pp. 46–72). IGI Global.
- ◆ Klaus, P., & Zaichkowsky, J. L. (2022). *The convenience of shopping via voice AI: Introducing AIDM*. *Journal of Retailing and Consumer Services*, 65, 102490.
- ◆ Olsen, G. D., & Pracejus, J. W. (2020). *Customized advertising: Allowing consumers to directly tailor messages leads to better outcomes for the brand*. *Journal of Business Research*, 116, 245–257.
- ◆ Van Esch, P., & Stewart Black, J. (2021). *Artificial intelligence (AI): revolutionizing digital marketing*. *Australasian Marketing Journal*, 29(3), 199–203.

Architecting an AI-Powered Decentralized Exchange: Integrating On-Chain Trading, Agentic Browsers, and Stablecoins for Autonomous Financial Services

MEHUL MANGAL¹

Student, Jamia Hamdard University,
New Delhi, India
Email: mehulmangal23@gmail.com

AYUSH KUMAR JHA²

Student, Jamia Hamdard University,
New Delhi, India
Email: ayushkmrjha@gmail.com

DR. IHTIRAM RAZA KHAN³

Honorary Adjunct Professor,
Jamia Hamdard University
Email: erkhan2007@gmail.com

Key Words: *Decentralized Finance (DeFi), AI-Powered DEX, Multi-Agent System, Maximal Extractable Value (MEV), Agentic Crypto Browser, Automated Market Maker (AMM).*

Abstract

Decentralized finance (DeFi) continues to evolve as an alternative financial paradigm that offers increased transparency and automated control when compared to traditional financial structures. Despite these advantages, several challenges still persist, including high transaction costs, fragmented liquidity, execution inefficiencies, and interference driven by Maximal Extractable Value (MEV). This research presents the architecture of an AI-enabled decentralized exchange (DEX) designed to address these limitations, particularly in high-friction execution environments. The proposed framework integrates a hybrid on-chain trading engine, a multi-agent intelligence system, and an intent-driven agentic browser interface. Stablecoin-based trading pairs are used to provide price stability, while AI-powered liquidity management help mitigate exposure to volatility-related risk. In addition, MEV-aware execution paths are incorporated to promote fairer transaction outcomes across decentralized markets. From a system-design perspective, this framework draws on insights from blockchain research, predictive analytics, smart-contract automation, and emerging decentralized user-interaction models. In practical terms, the study overall presents a functional and flexible blueprint for the next generation of autonomous and adaptable financial platforms, particularly those suited for emerging digital economies.

Introduction

Over the past few years, Decentralized finance (DeFi) has rapidly emerged as a transformative force within the modern financial ecosystem, fundamentally reshaping how financial services are accessed and delivered. By removing centralized intermediaries, DeFi enables users to retain direct control over their assets while engaging in transparent, permissionless, and borderless financial transactions. This shift has introduced a new level of openness and autonomy, making financial participation more inclusive and globally accessible. Within this ecosystem, decentralized exchanges (DEXs) play a foundational role, as they enable peer-to-peer trading on blockchain networks and often serve as the primary gateway to broader DeFi services (SoK: Decentralized Exchanges, 2021).

Despite their growing adoption, existing generations of DEXs continue to face a range of operational and technical challenges. On heavily utilized blockchain networks such as Ethereum, network congestion frequently leads to elevated gas fees and slower transaction confirmation times. These conditions increase execution costs and expose users—particularly retail participants and algorithmic traders—to heightened financial risk (OSL, 2023). Automated Market Makers (AMMs), which were

instrumental in enabling early decentralized trading, also present inherent limitations. Issues such as inefficient capital utilization, high slippage during large trades, and the risk of impermanent loss for liquidity providers remain persistent, especially during periods of market volatility (BIS, 2021).

As the DeFi landscape has expanded, liquidity fragmentation across multiple DEX platforms has become another critical concern. Liquidity dispersed among numerous protocols weakens effective price discovery and amplifies execution risk, particularly in volatile market conditions (BIS Working Paper, 2024). Under such circumstances, users are often required to balance competing factors—fees, transaction speed, liquidity depth, and slippage—across different platforms, which significantly increases decision-making complexity.

One of the most challenging structural issues affecting decentralized markets is Maximal Extractable Value (MEV). Because pending transactions are publicly visible in the blockchain mempool, malicious actors or block producers can manipulate transaction ordering to extract profit through front-running, back-running, or sandwich attacks (Chainlink, 2024). MEV is often described as an

“invisible tax” on users, as it degrades execution quality and undermines trust in the fairness and reliability of DeFi markets (Blockstream, 2022; Arkham Intelligence, 2025).

At the same time, advancements in artificial intelligence (AI) have significantly enhanced capabilities in data-driven decision-making, real-time analysis, and automated reasoning. Modern AI systems are increasingly capable of processing large volumes of on-chain and off-chain data, identifying patterns, forecasting market behavior, and executing complex strategies autonomously. Given the highly dynamic and data-intensive nature of DeFi environments, these capabilities present a natural and compelling opportunity for integration (MDPI, 2022).

In parallel, the user experience within DeFi is undergoing a notable transformation. Early DeFi interfaces required users to manually configure technical parameters such as slippage tolerance, gas fees, liquidity provision, and multi-step transaction workflows. More recently, intent-based interaction models have gained prominence. In these models, users simply express their objectives, while intelligent agents interpret those intentions and autonomously execute the necessary actions. This approach is increasingly recognized as a key design paradigm for improving accessibility and usability in decentralized systems (OSL, 2023). Motivated by these challenges and emerging opportunities, this paper proposes an advanced architecture for an AI-powered decentralized exchange. The proposed framework is structured around three core layers:

- A Hybrid On-Chain Settlement Layer, combining the continuous liquidity of AMMs with the precise price discovery of on-chain limit order books to improve execution efficiency and liquidity utilization.
- An Off-Chain Multi-Agent Intelligence Layer, composed of specialized AI agents responsible for smart order routing, predictive market-making, risk monitoring, and governance analysis.
- An Agentic Crypto Browser, designed to interpret user intent and translate it into optimized, automated blockchain interactions.

In addition, the framework emphasizes a stablecoin-based settlement model, as stablecoins reduce exposure to price volatility and provide more predictable execution outcomes (On-chain Analysis Study, 2023; OSL, 2023). By integrating hybrid trading mechanisms, autonomous AI agents, and intent-driven user interfaces, this architecture

envision a new generation of decentralized exchanges—one in which the DEX functions not merely as a passive execution venue, but as an intelligent and adaptive market system capable of actively understanding and fulfilling user objectives.

Background and Literature Review

A. The Evolution of On-Chain Trading Mechanisms

Decentralized exchanges have been central to the growth and maturity of the DeFi ecosystem. Their earliest designs were driven by a clear motivation: removing custodial dependence on centralized intermediaries and allowing users to trade directly from their own wallets. This shift significantly improved transparency and asset sovereignty. At the same time, however, early DEX implementations struggled to gain widespread adoption due to shallow liquidity, slow execution, and interfaces that were often difficult for non-expert users to understand.

The introduction of Automated Market Makers (AMMs) marked a turning point in decentralized trading. Rather than relying on traditional limit order books, AMMs used liquidity pools governed by predefined mathematical functions, enabling continuous trading without the need for active market makers (SoK: Decentralized Exchanges, 2021). Platforms such as Uniswap V2 demonstrated that decentralized liquidity could scale effectively, making on-chain trading more accessible and reducing friction for users.

As adoption increased, the limitations of AMM-based systems became more apparent. A key challenge lies in capital inefficiency. Because liquidity is distributed evenly across the price curve—even when trading activity is concentrated in narrow price ranges—large amounts of capital often remain underutilized (BIS, 2021). This design results in higher slippage for medium and large trades and exposes liquidity providers to impermanent loss, particularly during volatile market movements. Empirical studies indicate that such losses can substantially reduce returns for liquidity providers when markets experience sustained price swings (BIS Working Paper, 2024).

Network-level constraints further intensify these issues. On

congested blockchains like Ethereum, high gas fees discourage frequent liquidity adjustments, limiting providers' ability to actively manage positions. In response, concentrated liquidity models such as Uniswap V3 were introduced, allowing liquidity providers to deploy capital within specific price ranges. While this approach significantly improves efficiency, it also introduces added complexity. Managing concentrated positions requires deeper technical knowledge, effectively favoring professional market makers over casual participants (AMM-based DEX on XRP Ledger, 2023).

Alongside AMMs, fully on-chain limit order book (LOB) models have also shaped decentralized trading. Systems such as Serum, built on high-throughput networks like Solana, demonstrate that real-time order matching is possible on-chain. These models offer precise price discovery and support advanced order types, closely resembling centralized exchanges. However, they depend heavily on continuous market-making activity. If liquidity provision becomes concentrated among a small group of participants, concerns related to partial centralization may arise.

Given the trade-offs associated with both AMM and LOB designs, recent research has increasingly focused on hybrid models that combine their strengths. Hybrid architectures aim to preserve the continuous liquidity of AMMs while leveraging order books for improved execution accuracy. Smart Order Routing (SOR) mechanisms further enhance these systems by dynamically splitting trades across multiple liquidity sources to reduce slippage and execution costs (OSL, 2023).

Another critical dimension influencing on-chain trading design is Maximal Extractable Value (MEV). Because pending transactions are visible in public mempools, adversarial actors can manipulate transaction ordering through strategies such as front-running and sandwich attacks. Prior research consistently identifies MEV as a structural threat to fairness, efficiency, and user trust within decentralized markets (Chainlink, 2024; Blockstream, 2022; Arkham Intelligence, 2025).

Taken together, existing literature suggests that current on-chain trading mechanisms have reached the limits of purely static designs. The movement toward hybrid liquidity structures and intelligent execution reflects a broader need

for more adaptive, automated, and user-aware exchange infrastructures.

Table 1, which summarizes the comparative features of AMMs, concentrated liquidity AMMs, on-chain order books, and hybrid models, is provided in the table sheet.

B. The Emergence of Autonomous AI Agents in Decentralized Finance

The growing integration of artificial intelligence into decentralized finance has introduced a new layer of automation and adaptability. In traditional financial systems, tasks such as market analysis, risk monitoring, and strategic execution typically require human oversight or centralized tooling. DeFi, by contrast, is increasingly adopting autonomous AI agents that operate continuously across protocols, responding to market changes in real time (MDPI, 2022).

One of the defining strengths of autonomous agents is their ability to process large volumes of heterogeneous data simultaneously. These agents analyze on-chain transaction flows, off-chain market signals, and historical trends to identify patterns that would be difficult to detect manually. In fast-moving DeFi environments where liquidity, gas costs, and competition fluctuate rapidly—this capability enables more timely and precise decision-making.

AI agents have shown particular effectiveness in arbitrage detection and liquidity optimization. By monitoring price discrepancies across decentralized markets, agents can identify profitable opportunities and execute trades with minimal latency. Similarly, sudden liquidity imbalances can be detected early, allowing systems to rebalance pools or adjust strategies before risks escalate.

Predictive modeling further enhances agent performance. Machine learning techniques such as LSTM networks, regression models, and sentiment-driven analysis enable agents to forecast volatility, anticipate liquidity shifts, and identify scenarios likely to result in impermanent loss. These predictive insights support more informed liquidity allocation and help reduce risk exposure for market participants.

From a usability perspective, the rise of intent-based interaction represents a significant shift in how users engage with DeFi protocols. Instead of manually configuring technical parameters—such as slippage tolerance, gas prioritization, or routing paths—users can express high-level goals in natural language. AI agents then translate these intents into optimized execution strategies (OSL, 2023). This abstraction reduces cognitive load and lowers barriers to entry for non-technical users.

AI agents are also being applied to governance processes. Governance proposals in DeFi often involve complex economic and technical trade-offs that are difficult for participants to assess. Governance intelligence agents can summarize proposals, simulate potential outcomes, and highlight associated risks, supporting more informed community decision-making (arXiv, 2025). Importantly, these systems are designed to assist governance participants rather than replace human judgment.

Despite these advantages, challenges remain. Many AI-driven DeFi systems rely on off-chain computation or proprietary models, raising concerns related to transparency, decentralization, and adversarial manipulation. Addressing these concerns requires careful design choices that prioritize explainability, auditability, and robustness.

C. The Foundational Role of Stablecoins in DeFi Ecosystems

Stablecoins play a central role in the functionality and stability of decentralized finance. In markets characterized by frequent and sometimes extreme volatility, stablecoins provide a reliable medium of exchange and a consistent unit of account. This stability supports a wide range of DeFi activities, including trading, lending, liquidity provision, and automated strategy execution (MDPI, 2022; OSL, 2023).

Stablecoins generally fall into four categories: fiat-collateralized, crypto-collateralized, commodity-backed, and algorithmic models. Fiat-backed stablecoins, such as USDC, are widely used due to their price stability and relatively transparent reserve structures. However, their reliance on centralized custodians introduces counterparty and regulatory risks. Crypto-collateralized stablecoins,

while more decentralized, typically require over-collateralization, reducing capital efficiency and increasing sensitivity to market downturns (On-chain Analysis Study, 2023).

Commodity-backed stablecoins attempt to link digital assets to physical commodities, whereas algorithmic stablecoins rely on supply-adjustment mechanisms governed by code. Although algorithmic models aim to achieve full decentralization, historical failures during periods of market stress have raised serious concerns regarding their long-term viability (arXiv, 2025).

Within decentralized exchanges, stablecoins are particularly valuable. Trading pairs denominated in stable assets reduce slippage, improve price predictability, and lower risk exposure for both traders and liquidity providers. As a result, stablecoins are frequently used as base assets in AMM pools and routing strategies.

Stablecoins are also well-suited to AI-driven DeFi systems. Their relatively stable price behavior provides cleaner data for machine learning models, improving the reliability of forecasting, liquidity optimization, and risk assessment. In intent-based interfaces, stablecoins enable AI agents to design strategies that align closely with user preferences for safety and predictability.

As stablecoins become more deeply embedded in DeFi and autonomous financial systems, regulatory scrutiny continues to increase. Concerns related to reserve transparency, systemic risk, and operational resilience highlight the importance of robust stablecoin design. Overall, stablecoins function as the stabilizing backbone of decentralized markets, enabling both efficient trading and advanced AI-driven automation.

Proposed Architecture for an AI-Powered DEX

A. System Overview and Core Design Principles

Designing a next-generation decentralized exchange is not simply an exercise in improving existing mechanisms. It requires a broader rethinking of how decentralized markets behave, how users interact with them, and how intelligence

can be embedded without undermining trust. Traditional DEX platforms are largely execution-oriented, leaving users to interpret market signals, manage risk parameters, and navigate technical complexity on their own. The proposed AI-powered DEX architecture shifts this responsibility, framing the exchange as an adaptive and intelligent financial system that actively assists users while still respecting decentralization principles.

This architecture is shaped around four core design principles. Each principle addresses a specific limitation of existing systems, and together they define the structural foundation of the proposed framework.

1. Trust Minimization

At the core of decentralized systems lies the elimination of reliance on centralized intermediaries. The proposed architecture preserves this principle by ensuring that all critical operations like the asset custody, trade settlement, liquidity accounting, and fee distribution, are executed entirely on-chain through immutable smart contracts (SoK: Decentralized Exchanges, 2021). Trust is derived from cryptographic verification and transparent execution rather than from institutional authority. By anchoring financial finality on-chain, the system reduces exposure to external interference and central points of failure.

2. Intelligence and Adaptability

Most current DEX platforms operate using static, rule-based models that struggle to adapt when market conditions shift rapidly. The proposed architecture addresses this limitation by introducing an off-chain multi-agent intelligence layer. Within this layer, specialized AI agents continuously monitor market behavior, analyze risk indicators, and adjust strategies in near real time. These agents are capable of anticipating volatility, reallocating liquidity, and optimizing execution paths as conditions evolve (MDPI, 2022; OSL, 2023). As a result, the DEX no longer behaves as a passive marketplace, but rather as a system that can respond dynamically to changing environments.

3. User-Centric Abstraction

Complexity remains one of the most persistent barriers to DeFi adoption. Users are often required to manually configure parameters such as slippage limits, gas priority, liquidity ranges, and routing paths. The proposed

architecture reduces this burden through an intent-based interaction model. Instead of interacting with low-level settings, users express high-level goals—for example, minimizing execution cost or maximizing returns within a risk threshold—and intelligent agents translate these intents into executable strategies (OSL, 2023). This abstraction simplifies the user experience while preserving user control.

4. Modular Composability

Given the rapid pace of innovation in blockchain and AI research, architectural flexibility is essential. The proposed DEX adopts a modular design in which the on-chain settlement layer, off-chain intelligence layer, and user interaction layer function as loosely coupled components. This structure allows individual modules such as AI models, routing logic, oracle systems, or interface elements like these to be upgraded independently. As a result, the architecture can adapt to future regulatory changes, technical advances, or new research insights without disrupting the overall system.

B. The On-Chain Layer: Trust and Settlement

The on-chain layer forms the trust anchor of the proposed DEX architecture. It is responsible for enforcing transaction integrity, securing assets, and ensuring transparent settlement. While higher-level intelligence informs execution decisions, final authority remains with deterministic smart contract logic deployed on-chain. This layer integrates three primary components: a hybrid liquidity model, AI-enhanced smart contracts, and MEV-resistant execution mechanisms.

1. Hybrid Liquidity Model (AMM + LOB)

A central innovation of the proposed system is the integration of Automated Market Maker (AMM) and on-chain Limit Order Book (LOB) mechanisms. AMMs provide continuous liquidity, ensuring that trades can be executed even during periods of low activity. LOBs, on the other hand, enable more precise price discovery and support advanced order types.

In the hybrid configuration, AMMs act as the baseline liquidity layer, while the LOB supports users who require more granular execution control. Prior studies suggest that hybrid models improve market depth, reduce slippage, and better align the incentives of liquidity providers and active

traders (BIS, 2021; AMM-based DEX on XRP Ledger, 2023). When deployed on high-performance blockchains, this combination allows near-real-time updates without sacrificing decentralization.

2. AI-Enhanced Smart Contracts

Unlike traditional DEX designs, the proposed architecture incorporates AI-aware smart contracts that can adapt selected parameters based on validated external signals. These contracts do not execute arbitrary AI logic. Instead, they expose predefined functions that may be triggered by authorized AI agents or oracles. This design choice preserves determinism while allowing controlled adaptability.

AI-enabled contract functions include dynamic fee adjustments, liquidity range optimization, volatility-sensitive curve tuning, and automated circuit breaker activation during abnormal conditions. Embedding these adaptive hooks directly into smart contracts makes the system more responsive, while still maintaining transparency and auditability.

3. Stablecoin-Centered Settlement

Stablecoins play a central role in the on-chain settlement framework. By denominating most trading pairs in stable-value assets, the architecture reduces exposure to sudden price fluctuations and improves execution predictability. Stablecoin-based settlement offers several advantages, including reduced slippage, more consistent transaction costs, and a reliable data foundation for AI-driven optimization (On-chain Analysis Study, 2023; OSL, 2023).

4. MEV Mitigation and Fair-Ordering Mechanisms

MEV remains one of the most persistent inefficiencies in decentralized markets. To mitigate this risk, the proposed architecture integrates several MEV-resistant techniques. These include private transaction relays, batched execution windows, randomized transaction ordering, and encrypted order submission where supported (Chainlink, 2024; Blockstream, 2022; Arkham Intelligence, 2025). Together, these mechanisms reduce transaction predictability and limit opportunities for adversarial extraction. Proposed DEXs incorporate several advanced techniques designed to mitigate MEV:

i) Private Transaction Relays - Individual transactions are submitted through private channels instead of being exposed to a public mempool, so reducing the likelihood of front-running and sandwich attacks.

ii) Batched Execution Windows - Trades are executed in groups to make it difficult for attackers to guess transaction patterns.

iii) Randomized Transaction Ordering - Also Randomizing the order of transactions shortens the MEV exploitation because attackers cannot predict which transactions will receive priority.

iv) Encrypted Order Submission (Where Supported) - Some blockchain platforms support encrypted mempools, which can be used to provide additional privacy within the system.

All of these measures aim to ensure fairness, transparency, and security of transactions, thereby increasing user trust and making the entire DEX ecosystem more stable.

C. The Off-Chain Intelligence Layer: A Multi-Agent System (MAS)

The off-chain intelligence layer acts as the decision-making core of the proposed DEX architecture. Rather than functioning as a single monolithic intelligence component, this layer is structured as a coordinated Multi-Agent System (MAS), where each agent is responsible for a specific operational domain. By decomposing complex decision-making tasks into specialized roles, the system becomes more scalable, resilient, and easier to evolve over time.

Each agent operates independently but remains context-aware, continuously sharing signals and insights with other agents in the system. This coordination allows the DEX to respond to market changes in real time, while still maintaining stability and predictable behavior.

1. Smart Order Routing (SOR) Agent

The off-chain intelligence layer acts as the decision-making core of the proposed DEX architecture. Rather than functioning as a single monolithic intelligence component, this layer is structured as a coordinated Multi-Agent System (MAS), where each agent is responsible for a specific operational domain. By decomposing complex decision-making tasks into specialized roles, the system becomes more scalable, resilient, and easier to evolve over time.

Each agent operates independently but remains context-aware, continuously sharing signals and insights with other agents in the system. This coordination allows the DEX to respond to market changes in real time, while still maintaining stability and predictable behavior.

The SOR agent is responsible for the following tasks:

- The Real-time analysis of various on-chain and off-chain liquidity sources,
- splitting trades into the best possible routes,
- minimizing the slippage, Optimizing gas costs,
- And Selecting the safest execution route by comparing MEV risk.

2. Predictive Market-Making (PMM) Agent

Traditional AMM designs rely on static pricing curves that react only after market conditions change. The Predictive Market-Making (PMM) agent introduces forward-looking intelligence into liquidity management.

By analyzing historical price data, trading volumes, volatility indicators, and sentiment signals, the PMM agent forecasts near-term market behavior. Time-series forecasting models, including LSTM-based approaches, are used to anticipate liquidity demand and potential price movements. Based on these predictions, the agent adjusts liquidity ranges and fee parameters dynamically, aiming to improve capital efficiency while reducing impermanent loss for liquidity providers (BIS, 2021). This predictive approach makes AMM behavior more adaptive, rather than purely reactive.

This agent engages in the following analyses:

- Volatility forecasting is done using historical price data,
- identifying future trends through LSTM and other predictive ML models,
- predicting market direction by analyzing on-chain and social media sentiments,
- dynamic adjustment of liquidity ranges & optimizing fee tiers to minimize impermanent losses.

3. Risk Monitoring & Security Agent

Security remains one of the most critical challenges in decentralized systems. The Risk Monitoring and Security Agent continuously observes transaction flows, oracle price feeds, liquidity movements, and smart contract interactions

across the protocol.

This agent applies anomaly detection techniques to identify suspicious behavior, such as flash-loan exploitation patterns, abnormal liquidity withdrawals, or unexpected oracle deviations. When predefined risk thresholds are exceeded, the agent can trigger circuit breakers, pause specific contract functions, or alert governance participants for further review. This design aligns with best practices highlighted in DeFi security research, where rapid detection and response are essential to limiting systemic damage (SoK: Decentralized Exchanges, 2021).

This agent performs the following functions:

- Continuously monitoring oracle price deviations,
- identifying unusual liquidity outflows or large transaction patterns,
- investigating signs of flash-loan-based attacks & ml-based anomaly detection to identify contract-level vulnerabilities,
- automatically activating circuit breakers when thresholds are exceeded,
- alerts users or governance to all suspicious activity.

4. Governance Intelligence Agent

Decentralized governance introduces transparency, but it also increases cognitive load for participants. Governance proposals often involve complex technical, economic, and security implications that are difficult to evaluate without specialized expertise.

The Governance Intelligence Agent addresses this challenge by applying natural language processing (NLP) techniques to summarize governance proposals and extract key changes. It also runs simulations to estimate potential economic impacts and identifies long-term risk indicators associated with proposed updates. While final decisions always remain with the community, this agent provides structured insights that improve decision quality and reduce information asymmetry among voters (arXiv, 2025).

This agent:

- Creates NLP-based summaries of proposals, runs simulations of potential impacts,
- calculates long-term risk indicators & comparatively evaluates the benefits and risks of a proposal in various

different scenarios,

- provides concise and clear recommendations to governance voters (arXiv, 2025).

Table 2 is a structured overview of the agents and also their functional roles is provided in the table sheet.

D. The User Interaction Layer: The Agentic Crypto Browser

The final and crucial component of the proposed AI-powered DEX architecture is the User Interaction Layer, specifically designed as an agentic crypto browser. This layer aims to make the user experience completely simple, intuitive, and intent-driven and while traditional DeFi interfaces required users to manually handle numerous complex steps such as swaps, liquidity management, gas settings, and protocol interactions, the agentic browser greatly streamlines and automates DeFi interactions. This layer aims to make DeFi accessible even to users who lack technical expertise but wish to access secure, efficient, and customized financial services.

1. Intent Translation

Instead of manually configuring parameters such as slippage limits, gas priority, or routing preferences, users express their objectives in natural language. Examples include allocating funds to low-risk strategies or identifying the most cost-efficient swap route for a given asset.

The agentic browser interprets these inputs using NLP models and forwards them to the Multi-Agent System. Each agent evaluates the request from its perspective—considering risk, cost, liquidity, and execution quality—before a consolidated strategy is presented to the user (OSL, 2023). This translation layer significantly simplify the user experience without removing user control.

This process involves:

- NLP-based analysis to understand the user's intent,
- evaluating all applicable DeFi protocols and available opportunities,
- comparing risk, cost, and execution quality,
- and then selecting the best strategy (OSL, 2023).

2. Execution Automation

Once the user approves a proposed strategy, execution is handled automatically by the system. This includes performing swaps, adjusting liquidity positions, optimizing gas usage, and coordinating cross-chain interactions when required.

Automation reduces the likelihood of user error and ensures consistent execution quality, particularly in time-sensitive scenarios. At each step, the system maintains transparency by displaying execution details and risk indicators, so users remain informed about what is happening and why. However, in this agentic model, AI agents automatically complete many tasks, including:

- token swaps, liquidity adjustments,
- staking or unstaking, gas efficiency optimization,
- yield generation strategies,
- and cross-chain bridging.

3. Donut-Style Agentic Browser

The concept of an agentic browser is currently emerging and should be viewed primarily as a theoretical or conceptual framework. Platforms like Solana-based Donut are referenced solely to demonstrate how integrated wallet management, DEX connectivity, real-time analytics, and AI-driven decision-making could be organized within a single interface in the future (OSL, 2023). However, it is important to note that the agentic crypto browser described in this architecture is conceptual. References to emerging platforms or experimental interfaces are included to illustrate design direction rather than to imply the existence of a fully deployed product. The browser should be understood as a forward-looking interaction model that reflects ongoing research and early experimentation in intent-based financial interfaces.

Key envisioned features of such a potential browser include:

- Integrated wallet management within the browser,
- real-time analysis of all liquidity and routing data,
- seamless connectivity with various DEXs.

And AI agents that automatically generate suggestions and

strategies based on user intent. The agentic browser concept described in the proposed DEX architecture draws inspiration from such early examples, but is designed to be more comprehensive, multi-agent-supported, and optimized for hybrid DEX operations and hence this reflects the future direction of the company/project currently under development, not the availability of any current product.

4. Trust-Alignment

To build and maintain user trust, the agentic browser provides clear explanations alongside every automated action. These explanations describe the reasoning behind selected strategies, highlight associated risks, and clarify expected outcomes and this ensures that automation enhances user confidence rather than obscuring system behavior so by keeping users informed and aligned with system decisions, the architecture reinforces trust in autonomous, AI-driven DeFi systems.

This ensures that:

- The rationale behind any transaction or strategy is clearly understood by the user,
- risk assessments are presented in a simple format,
- and the system never deviates from user intentions.

This trust-alignment model aims to make the user feel in control even if most technical tasks are handled autonomously by AI agents and this feature not only increases transparency but is also crucial for building trust in DeFi, especially for user who are first utilizing autonomous financial systems.

Security, Risk, and Ethical Considerations

Combining blockchain infrastructure with advanced multi-agent intelligence systems opens up new possibilities for automation, efficiency, and adaptability, but it also expands the system's attack surface and increases ethical complexities. As decentralized exchanges become more sophisticated, security structures must also evolve at the same pace. So This section discusses the key risks associated with smart contracts, oracles, AI agents, MEV dynamics, and protocol governance, as well as measures suggested by modern research to mitigate those risks.

A. Smart Contract and Oracle Security Framework

Smart contracts form the foundational layer of trust for any decentralized exchange, but their immutability also makes them a critical point of failure when flaws exist. Once deployed, vulnerabilities such as re-entrancy, unchecked external calls, flawed state transitions, or inadequate access controls cannot be easily corrected. Historical evidence across DeFi ecosystems shows that even minor oversights at the contract level have resulted in severe financial losses and, in some cases, complete protocol collapse. For this reason, the Systematization of Knowledge (SoK) on decentralized exchanges emphasizes that contract-level weaknesses remain among the most common and costly failure vectors in decentralized markets (SoK: Decentralized Exchanges, 2021).

To mitigate these risks, modern DeFi systems increasingly rely on layered security practices. These include formal verification, multi-stage security audits, adversarial testing, and minimizing contract complexity wherever possible. The proposed architecture follows these established best practices, ensuring that critical financial logic is both verifiable and resistant to common exploit patterns. In particular, contract functions that influence liquidity, settlement, or fee logic are deliberately constrained to reduce unintended behavior.

Oracle security represents another major challenge. Because decentralized exchanges depend on external data feeds for pricing and market information, oracles introduce a trust boundary between off-chain data and on-chain execution. Attackers can exploit this boundary by manipulating prices in low-liquidity markets, often through flash loans, causing oracles to report distorted values. Such manipulations can trigger mispriced trades, incorrect liquidations, or cascading protocol failures. BIS research highlights oracle dependence as a systemic risk, especially when protocols rely on single-source or non-time-weighted pricing mechanisms (BIS, 2021; BIS Working Paper, 2024).

To address oracle-related vulnerabilities, the proposed DEX architecture integrates decentralized oracle networks (DONs), time-weighted average price (TWAP) mechanisms, and cross-source validation. Price feeds are compared across multiple sources, and acceptable deviation thresholds are enforced before updates are accepted on-

chain. In addition, the Risk Monitoring Agent continuously evaluates oracle consistency and market conditions. When anomalies exceed predefined limits, the system may temporarily restrict sensitive operations or activate circuit breakers. This rapid-response capability is essential, as delayed intervention often amplifies losses during oracle-based attacks.

Overall, by combining robust smart contract design with layered oracle validation and continuous monitoring, the architecture aims to reduce both the likelihood and impact of high-severity exploits. While no system can be entirely risk-free, these measures significantly strengthen the protocol's defensive posture.

B. MEV, Execution Fairness, and Transaction Integrity

Maximal Extractable Value (MEV) remains one of the most persistent inefficiencies in decentralized markets. Because pending transactions are visible in public mempools, adversarial actors can observe user activity and strategically reorder, insert, or replicate transactions for profit. Common MEV strategies include front-running, back-running, and sandwich attacks, all of which degrade execution quality for ordinary users. Chainlink (2024) describes MEV as a structural consequence of transparent transaction ordering, while Blockstream (2022) highlights its long-term implications for market fairness and user trust.

The architecture proposed in this research addresses MEV not as a single-point vulnerability, but as a systemic risk that requires layered mitigation. One key strategy involves the use of private transaction relays, which prevent transactions from being exposed in the public mempool prior to execution. By limiting visibility, these relays reduce opportunities for searchers to exploit transaction ordering. In addition, batch-based execution windows are used to group transactions together, making individual order flows more difficult to predict.

Randomized transaction ordering further strengthens execution fairness. When the order of transactions within a batch is partially randomized, attackers cannot reliably anticipate which transactions will receive priority. On blockchains that support encrypted mempools, encrypted order submission adds an additional layer of protection by concealing transaction details until execution. Together,

these techniques reduce MEV extraction without requiring changes to core consensus mechanisms (Chainlink, 2024; Arkham Intelligence, 2025).

The Smart Order Routing (SOR) agent also contributes indirectly to MEV mitigation. By selecting execution paths with lower historical MEV exposure and avoiding predictable routing patterns, the agent helps stabilize execution outcomes. This adaptive behavior becomes especially important when AI agents automate trading strategies, since predictable patterns can be exploited more easily by adversarial searchers.

Execution fairness is not only a technical concern but also a trust issue. When users consistently experience degraded execution due to MEV, confidence in decentralized systems erode over time. By embedding MEV-resistant mechanisms directly into the execution layer, the proposed architecture aims to ensure that transaction integrity and fairness are treated as core design principles rather than optional optimizations.

C. AI-Specific Risks: Bias, Explainability, and Adversarial Attacks

The integration of artificial intelligence into decentralized financial infrastructure introduces a distinct category of risks that extend beyond traditional blockchain security concerns. Unlike deterministic smart contracts, AI systems rely on probabilistic models trained on historical data. As a result, their behavior can be influenced by biases embedded in training datasets, model assumptions, or evolving market conditions. In financial contexts, such biases may manifest in uneven liquidity allocation, routing preferences that favor specific assets, or inconsistent risk scoring across similar scenarios.

Research in AI-driven financial systems highlights that model bias is often unintentional, emerging from incomplete or non-representative data rather than explicit design choices (MDPI, 2022). In decentralized environments, where AI agents may directly influence execution outcomes, such biases can have tangible economic consequences. This becomes particularly important when agents operate continuously and at scale, since even small distortions can compound over time.

Explainability presents another significant challenge. If users are unable to understand why a particular action was taken, such as a trade route being selected or a liquidity position being adjusted, then the trust in the system can gradually diminish. To address this issue, the proposed architecture incorporates explainability-by-design. AI agents are required to generate human-readable explanations that describe the reasoning behind key decisions, especially when those decisions involve risk trade-offs or automated adjustments. This approach aligns with responsible AI guidelines that emphasize transparency and accountability in automated systems (OSL, 2023).

Adversarial attacks further complicate the deployment of AI in DeFi. Attackers may attempt to manipulate input data, exploit model weaknesses, or introduce adversarial patterns that mislead agent behavior. For example, coordinated transactions could be designed to distort short-term signals used by predictive models. To mitigate such threats, the architecture integrates adversarial robustness testing, continuous model validation, and agent-level anomaly detection. These safeguards help ensure that AI agents remain resilient even when operating in adversarial and rapidly changing environments (arXiv, 2025).

Overall, while AI agents introduce powerful capabilities, they also demand careful oversight. Addressing bias, ensuring explainability, and defending against adversarial manipulation are essential to maintaining trust and stability in intelligent decentralized systems.

D. Governance Risks and Protocol Decision-Making

Decentralized governance is often viewed as a strength of DeFi systems, but it also introduces a distinct set of risks. Governance decisions frequently involve complex technical upgrades, economic parameter changes, or modifications to security assumptions. For many participants, evaluating the full implications of such proposals can be challenging, especially when information is fragmented or highly technical in nature.

One major governance risk arises from information asymmetry. Large token holders or technically sophisticated participants may possess a deeper understanding of proposals, while smaller holders rely on limited summaries or community discussion. This

imbalance can influence voting outcomes in ways that are not always aligned with the broader interests of the protocol. In addition, voting apathy remains a persistent issue, allowing a relatively small subset of participants to shape critical decisions.

There is also the risk of governance capture, where actors accumulate sufficient voting power to pass proposals that benefit themselves at the expense of protocol stability. Historical incidents across DeFi ecosystems demonstrate that seemingly minor parameter changes—such as fee adjustments or oracle source modifications—can lead to significant downstream consequences when not carefully evaluated.

To address these challenges, the proposed architecture incorporates a Governance Intelligence Agent. This agent applies natural language processing techniques to summarize proposals, identify key changes, and highlight potential risks. It also performs simulations to estimate economic impacts under different scenarios, providing participants with structured insights rather than raw proposal text. While final authority remains with human voters, this support mechanism helps reduce information gaps and improve decision quality (arXiv, 2025).

Additional safeguards, such as time-locked execution and multi-signature approval mechanisms, further strengthen governance robustness. Time locks provide a buffer period between proposal approval and execution, allowing the community to react if unintended risks are identified. Together, these measures aim to balance decentralization with informed oversight, ensuring that governance remains both participatory and resilient.

E. Ethical and Regulatory Considerations

The convergence of artificial intelligence and decentralized finance introduces ethical considerations that extend beyond technical security and performance. As AI agents gain greater autonomy in executing financial actions, questions arise regarding accountability, user protection, and the appropriate boundaries of automated decision-making. Unlike traditional financial systems, where responsibility can often be traced to centralized institutions, DeFi systems distribute control across code, governance mechanisms, and autonomous agents, which complicate

ethical oversight.

One ethical concern relates to user protection. AI-driven systems may optimize for efficiency or profitability, but these objectives do not always align perfectly with user understanding or expectations. For example, an automated strategy might technically satisfy a stated intent while exposing users to risks they did not fully anticipate. This makes transparency and explainability especially important. The proposed architecture addresses this issue by requiring AI agents to provide clear explanations and risk indicators alongside automated actions, ensuring that users remain informed and able to intervene when needed. Another ethical dimension involves the limits of autonomy. While automation can improve efficiency and reduce human error, fully autonomous financial decision-making raises concerns about loss of user agency. For this reason, the architecture is designed so that AI agents assist rather than replace human intent. Critical actions require explicit user approval, and the system is constrained to operate within predefined boundaries aligned with user goals. This design choice reflects broader ethical principles in responsible AI deployment, where human oversight remain a central requirement.

Regulatory considerations also play an increasingly important role. Global regulatory bodies have expressed growing interest in DeFi systems, particularly those that incorporate advanced automation and AI. Issues such as anti-money laundering (AML), know-your-customer (KYC) requirements, consumer protection, and systemic risk are becoming more prominent in regulatory discussions. Industry analyses suggest that intelligent DeFi systems may eventually be required to integrate risk-based monitoring, anomaly detection, and selective compliance mechanisms (OSL, 2023).

The proposed architecture adopts a hybrid compliance approach. Core trading and settlement functions remain permissionless and decentralized, preserving the foundational principles of DeFi. However, optional layers—such as decentralized identity frameworks or enhanced monitoring modules—can be activated in higher-risk scenarios. This flexible design allows the system to adapt to evolving regulatory expectations without imposing blanket restrictions on all users. By balancing decentralization with ethical responsibility and regulatory awareness, the architecture aims to support sustainable long-term adoption.

Table 3 summarizes these security threats and mitigation strategies in the proposed architecture in the table sheet.

F. Empirical Risk Analysis: Lessons from Recent DeFi Incidents

Although the proposed AI-powered DEX architecture is conceptual, empirical analysis of past DeFi incidents provides valuable insight into the real-world risks such systems may face. Historical data consistently shows that the most damaging failures in decentralized finance arise from a small number of recurring vectors—namely smart contract vulnerabilities, oracle manipulation, and MEV-based exploitation (SoK: Decentralized Exchanges, 2021; BIS, 2021).

Smart contract failures remain a leading cause of protocol losses. Issues such as re-entrancy attacks, unchecked external calls, and flawed state-transition logic have resulted in rapid and large-scale fund depletion. These vulnerabilities are often exploited by automated bots that operate continuously and react faster than human operators. The impact of such exploits is magnified in highly composable DeFi environments, where a single failure can cascade across interconnected protocols. This historical pattern reinforces the importance of formal verification, minimal contract design, and automated monitoring, all of which are integrated into the proposed architecture.

Oracle manipulation represents another well-documented risk. Numerous incidents have involved attackers using flash loans to temporarily distort asset prices in low-liquidity markets, causing oracles to report inaccurate values. These distorted prices have triggered improper liquidations, mispriced trades, and protocol insolvency. BIS research highlights that protocols relying on single-source or non-time-weighted oracles are particularly vulnerable to such attacks (BIS Working Paper, 2024; Chainlink, 2024). As a result, the architecture emphasizes decentralized oracle networks, cross-validation, and time-weighted pricing as essential safeguards.

MEV exploitation has also extracted significant value from users over time. Data presented by Arkham Intelligence (2025) indicates that sandwich attacks and priority gas auctions have removed hundreds of millions of dollars from user transactions. These losses, while individually small in

many cases, accumulate at scale and undermine confidence in decentralized markets. The empirical prevalence of MEV attacks underscores the need to integrate MEV-resistant execution mechanisms directly into system design, rather than treating them as optional enhancements.

These historical incidents demonstrate that the risks addressed in this architecture are not hypothetical. By incorporating AI-enhanced monitoring, oracle safeguards, MEV mitigation techniques, and governance support mechanisms, the proposed framework directly responds to the most common and costly failure scenarios observed in real-world DeFi systems. While no architecture can eliminate all risk, learning from empirical evidence significantly improves the likelihood of building resilient and trustworthy decentralized exchanges.

Practical Applicability & Industry Implications

The proposed AI-powered decentralized exchange, while still conceptual and under development, offers immense practical potential given the current blockchain ecosystem's evolution. As blockchain networks progress towards higher throughput, lower latency, and mature developer tooling, this architecture is becoming more suitable for practical deployment. The combination of a hybrid settlement model, a multi-agent intelligence layer, and an intent-driven interface addresses key issues clearly identified in the development of existing DEX platforms (SoK: Decentralized Exchanges, 2021). Thus, this conceptual model provides the foundation for future advanced exchanges that will be more intelligent, secure, and user-centric.

1. Applicability Across Blockchain Ecosystems

Although the proposed AI-powered decentralized exchange remains conceptual, its design aligns closely with the current trajectory of blockchain infrastructure development. As blockchain networks continue to evolve toward higher throughput, lower latency, and improved developer tooling, the practical feasibility of such architectures increases significantly. The combination of hybrid settlement mechanisms, multi-agent intelligence, and intent-driven interaction addresses limitations that have been widely observed in existing DEX platforms (SoK: Decentralized Exchanges, 2021).

High-performance blockchain ecosystems such as Solana, Aptos, and Sui are particularly well-suited for hybrid AMM–order-book architectures. These networks offer fast block times and low transaction latency, enabling near–real-time order matching and frequent liquidity updates without degrading user experience. Such performance characteristics are critical for intelligent routing, predictive liquidity management, and continuous agent-based analytics, all of which depend on timely data and rapid execution.

Ethereum Layer-2 solutions, including Arbitrum and Optimism, also present a viable environment for deploying this architecture. By reducing transaction costs and improving execution predictability, these networks allow AI agents to operate more efficiently without imposing excessive fees on users (OSL, 2023). In these contexts, the Multi-Agent System can analyze liquidity conditions across multiple chains, dynamically select optimal execution routes, and adjust strategies based on cross-chain opportunities. This becomes increasingly relevant as DeFi ecosystems move toward a multi-chain and interoperable future.

Stablecoins play a particularly important role in enabling cross-ecosystem applicability. Because a large proportion of DeFi activity already relies on stable-value assets, stablecoin-based settlement provides a consistent pricing reference across different networks (On-chain Analysis Study, 2023). For AI agents, this stability simplifies forecasting and risk assessment, making automated decision-making more reliable. As a result, the proposed architecture is not limited to a single blockchain environment, but can adapt to a wide range of network conditions and performance profiles.

2. Implications for Liquidity Providers and Market Makers

Liquidity providers (LPs) are central to the functioning of decentralized exchanges, yet they often face operational challenges that limit participation. Monitoring price movements, adjusting liquidity ranges, and managing impermanent loss require continuous attention and technical expertise. Research on AMM-based systems shows that passive liquidity provision, without active management, can significantly reduce capital efficiency and long-term returns (BIS, 2021).

The proposed architecture addresses these challenges through the Predictive Market-Making (PMM) agent. By continuously analyzing volatility, historical price patterns, and liquidity demand, the PMM agent can automatically rebalance liquidity positions in response to changing market conditions. This reduces the need for manual intervention and allows LPs to participate more effectively without constant monitoring. For many participants, this automation lowers the entry barrier to providing liquidity in complex DeFi environments.

Professional market makers also benefit from the hybrid design. The presence of an on-chain order-book component allows for more sophisticated trading strategies, including limit orders and tighter spread management. At the same time, AI-driven risk analysis provides additional insight into exposure management and execution quality. This combination makes the architecture attractive to both passive LPs and active market participants, increasing overall liquidity depth. As liquidity becomes more efficiently allocated, markets benefit from reduced slippage and improved price stability. Over time, these effects can contribute to healthier trading environments, where both retail and professional participants experience more predictable outcomes. The architecture thus aligns the incentives of liquidity providers, traders, and the protocol itself.

3. Implications for Retail Users

For retail users, complexity remains one of the most significant barriers to participating in decentralized finance. Traditional DEX interfaces often require users to understand technical concepts such as slippage tolerance, gas optimization, routing decisions, and liquidity mechanics. These requirements can discourage participation or lead to costly mistakes, particularly for users with limited technical backgrounds.

The proposed agentic browser fundamentally changes this interaction model. Instead of managing low-level parameters, users communicate their objectives in simple natural language. Examples include requests such as swapping assets at the lowest possible fee, allocating capital to low-risk stablecoin strategies, or rebalancing a portfolio at regular intervals. The Multi-Agent System interprets these instructions and automatically executes the necessary steps on behalf of the user. This abstraction significantly

reduces cognitive load and improves accessibility. By automating complex backend processes, the system minimizes the likelihood of user error while improving execution quality. Importantly, the architecture maintains transparency by presenting users with clear explanations and risk indicators before execution. Users remain informed and in control, even though many technical tasks are handled autonomously.

From an adoption perspective, this approach aligns with broader trends in the Web3 ecosystem, where intent-based interactions are increasingly viewed as essential for reaching a wider audience (OSL, 2023). By simplifying user experience without sacrificing decentralization or security, the proposed architecture has the potential to make DeFi more inclusive and user-friendly for everyday participants.

4. Institutional and Enterprise Applications

Institutional participation in decentralized finance depends heavily on transparency, predictability, and governance rigor. Unlike retail users, institutions typically operate under strict compliance requirements and require systems that support auditability, risk controls, and structured decision-making. The proposed AI-powered DEX architecture aligns well with these expectations by combining on-chain settlement with automated monitoring and governance intelligence.

One of the primary advantages for institutional users lies in transparent settlement. Because all critical transactions are finalized on-chain, institutions can audit execution paths, verify asset custody, and track fee flows with a high degree of confidence. Stablecoin-based valuation further enhances this transparency by reducing exposure to short-term volatility and simplifying accounting processes. For institutions exploring tokenized assets or automated settlement pipelines, this consistency is particularly valuable.

Automated risk management is another important factor. The inclusion of dedicated risk monitoring agents enables continuous surveillance of market conditions, oracle behavior, and protocol health. Rather than relying solely on periodic manual reviews, institutions benefit from real-time alerts and predefined safety mechanisms. This capability becomes especially relevant in volatile environments, where delayed response can significantly amplify losses. The architecture therefore supports a more proactive risk

posture, which aligns with institutional risk management frameworks. Governance intelligence also plays a meaningful role in institutional adoption. Governance proposals in DeFi often introduce changes to economic parameters, security assumptions, or protocol architecture. Evaluating these proposals requires technical expertise and time, both of which may be limited in enterprise settings. The Governance Intelligence Agent addresses this challenge by summarizing proposals, simulating potential impacts, and highlighting risk indicators in a structured format (arXiv, 2025). While final decisions remain with governance participants, this support layer reduces analysis overhead and improves decision confidence.

5. Broader Market Implications

Beyond individual user groups, the adoption of AI-powered, agent-driven DEX architectures could have far-reaching implications for the broader DeFi ecosystem. Features such as intelligent liquidity allocation, MEV-resistant execution, and intent-based interaction collectively address many of the structural weaknesses that have historically limited decentralized market efficiency.

From a market stability perspective, automated liquidity management and predictive fee adjustments can reduce extreme price swings and improve depth during periods of volatility. By responding dynamically to changing conditions, AI agents help smooth short-term imbalances that might otherwise lead to sharp execution inefficiencies. Over time, this contributes to more reliable price discovery and healthier trading environments.

Execution fairness is another important implication. MEV-resistant mechanisms—such as private transaction relays and randomized ordering—reduce the value extracted by adversarial actors at the expense of ordinary users (Chainlink, 2024). As these protections become embedded at the architectural level, user trust in decentralized markets may improve. This is particularly important for long-term adoption, since persistent execution disadvantages tend to discourage participation by less sophisticated users.

The introduction of agentic interfaces also has inclusivity implications. By lowering technical barriers, intent-based systems allow a broader range of participants to engage with DeFi without requiring deep protocol knowledge. This shift could expand the user base beyond technically proficient early adopters, increasing diversity and participation across

different demographic groups. As more users are able to interact safely and efficiently, network effects may further strengthen liquidity and market depth. At an industry level, widespread adoption of such architectures could influence design standards across DEX platforms. As users come to expect intelligent routing, automated risk controls, and transparent explanations, competitive pressure may drive other protocols to adopt similar approaches. In this sense, the proposed architecture not only represents a single system design, but also signals a broader direction for the evolution of decentralized exchanges toward more adaptive, user-centric, and resilient market infrastructure.

Conceptual Case Study: Illustrating an Intent-Based Workflow

This conceptual case study is intended to illustrate how the proposed AI-powered decentralized exchange architecture could operate in practice. Rather than claiming real-world deployment or performance outcomes, the purpose of this example is to demonstrate how user intent, multi-agent coordination, and intelligent execution mechanisms interact within the system. The scenario highlights how intent-driven interaction can simplify complex DeFi workflows while maintaining security, transparency, and efficiency.

Scenario Overview

Consider a user, Ananya, who wishes to generate stable, low-risk returns on an investment of 10,000 USDC. She prefers to avoid volatile assets and does not want to manually interact with multiple DeFi protocols. Managing liquidity positions, routing swaps, and monitoring protocol risk would require constant attention, which she aims to minimize. To achieve this, Ananya uses an agentic crypto browser connected directly to the Multi-Agent System (MAS) of the proposed DEX.

The browser provides a simple, intent-based interface. Instead of navigating technical settings, Ananya only needs to describe her objective clearly, allowing the system to interpret and execute the strategy on her behalf.

Step 1: User Intent and Interpretation

Ananya enters the following instruction into the browser interface: “Generate low-risk returns on my 10,000 USDC and avoid volatile assets.”

Once this instruction is submitted, the agentic browser forwards the intent to the MAS, where it is interpreted by multiple specialized agents. Each agent evaluates the request from its own perspective:

- The Predictive Market-Making (PMM) agent analyzes historical volatility, impermanent loss patterns, and average returns associated with stablecoin liquidity pools (BIS, 2021).
- The Smart Order Routing (SOR) agent examines available execution routes, focusing on fee efficiency, liquidity depth, and execution reliability.
- The Risk Monitoring Agent evaluates oracle stability, recent flash-loan activity, and the security posture of candidate protocols (OSL, 2023).

Through this coordinated analysis, the system translates a high-level user goal into a structured set of actionable constraints. This step is critical, as it ensures that automated execution remains aligned with the user’s risk tolerance and preferences.

Step 2: Strategy Construction

Based on the combined analysis of the agents, the MAS constructs a strategy tailored to Ananya’s objectives. To reduce dependency on a single asset, the system first recommends splitting the 10,000 USDC across two reputable stablecoin representations. This diversification helps mitigate asset-specific risks, even within a stable-value framework.

The system then identifies a stablecoin AMM pool with a strong security history, consistent yields, and sufficient liquidity depth (On-chain Analysis Study, 2023). Before deploying funds, the PMM agent adjusts liquidity ranges based on current volatility forecasts, aiming to reduce the likelihood of impermanent loss. At the same time, the Risk Monitoring Agent recommends activating safety mechanisms that can pause or rebalance positions if predefined risk thresholds are crossed.

Throughout this process, the browser presents Ananya with clear explanations of the proposed actions. Although the

system automates strategy construction, user visibility remain a priority, ensuring that decisions are understandable rather than opaque.

Step 3: Execution

After reviewing and approving the proposed strategy, Ananya authorizes execution. At this stage, the SOR agent performs the necessary swaps, selecting routes that minimize fees and slippage. The PMM agent deploys liquidity according to its predictive model, adjusting parameters dynamically to reflect current market conditions.

All transactions are submitted using MEV-resistant execution pathways, which may include private relays, batch execution, and randomized transaction ordering. These mechanisms reduce the likelihood of front-running or sandwich attacks, resulting in more predictable outcomes for the user (Chainlink, 2024). During execution, the Risk Monitoring Agent continues to observe protocol behavior, ready to intervene if abnormal conditions arise.

This automated execution phase highlights how complex, multi-step DeFi actions can be carried out with minimal user intervention, without sacrificing safety or execution quality.

Step 4: Ongoing Adaptation

Following execution, the MAS continues to monitor both the deployed strategy and broader market conditions. If minor volatility is detected within the stablecoin pool, the PMM agent may widen liquidity ranges to reduce exposure. If oracle deviations or unusual transaction patterns are observed, the Risk Monitoring Agent can trigger alerts or initiate protective measures.

In parallel, the Governance Intelligence Agent monitors governance activity related to the underlying protocol. If a proposal is detected that could materially increase risk—such as changes to fee structures or oracle sources—the agent prepares a concise summary and notifies Ananya. This allows her to remain informed without actively tracking governance forums.

These adaptive responses demonstrate how the system prioritizes user safety while remaining flexible. The architecture does not rely on static assumptions, but instead adjusts continuously as conditions evolve.

Outcome

At the conclusion of this conceptual scenario, Ananya achieves her objective of earning stable returns with minimal operational overhead. The coordinated behavior of the MAS, combined with intent-based interaction and MEV-aware execution, illustrates how advanced automation can make DeFi more accessible and reliable.

While this case study is illustrative rather than empirical, it demonstrates the practical value of intent-driven workflows. By reducing complexity, improving execution fairness, and maintaining transparency, the proposed architecture shows how AI-powered DEX systems could deliver more equitable and user-centric financial services in real-world settings.

Conclusion

This research presents a conceptual architecture for an AI-powered decentralized exchange that aims to address several long-standing limitations within existing DeFi systems. While decentralized exchanges have successfully introduced transparency, self-custody, and permissionless access, they continue to face challenges related to capital inefficiency, MEV-based exploitation, user complexity, and governance asymmetries. The architecture proposed in this study outlines a structured approach for integrating hybrid on-chain trading mechanisms, multi-agent intelligence, and intent-driven user interaction to respond to these challenges in a coherent manner.

A central contribution of this work lies in the integration of Automated Market Makers and on-chain order-book models into a unified hybrid framework. By combining continuous liquidity with precise price discovery, the architecture seeks to improve execution quality while balancing the needs of both passive liquidity providers and active traders. The use of stablecoin-centered settlement further enhances predictability, offering a more reliable foundation for both users and AI-driven optimization

processes. This stability becomes especially important when intelligent agents are responsible for forecasting, routing, and risk management decisions.

The multi-agent system (MAS) forms the analytical core of the proposed DEX. Each agent—whether focused on smart order routing, predictive market-making, risk monitoring, or governance analysis—contributes a specialized perspective while operating within a coordinated framework. This division of responsibilities allows the system to adapt dynamically to changing market conditions, rather than relying on static rule-based behavior. As demonstrated through the conceptual case study, such coordination enables complex financial workflows to be executed with reduced user burden and improved execution fairness.

User interaction is reimagined through an agentic crypto browser that emphasizes intent-based communication. By allowing users to express goals instead of configuring technical parameters, the architecture lowers cognitive barriers and makes DeFi more accessible to a broader audience. Importantly, this abstraction does not remove user control. Instead, transparency and explainability are maintained through clear strategy explanations and risk indicators, ensuring that automation support user decision-making rather than replace it.

Security, ethics, and governance considerations are treated as foundational elements rather than afterthoughts. The architecture incorporates layered defenses against smart contract vulnerabilities, oracle manipulation, and MEV exploitation, while also addressing AI-specific risks such as bias and adversarial behavior. Governance intelligence mechanisms further support informed participation, helping mitigate risks associated with information asymmetry and governance capture. While no system can eliminate risk entirely, these design choices reflect lessons drawn from empirical DeFi failures and current best practices.

It is important to note that this research remains conceptual in nature. The architecture described has not yet been implemented or evaluated under real-world conditions, and practical deployment would introduce additional challenges related to scalability, regulatory compliance, and operational complexity. However, the framework provides a clear blueprint for future experimentation and

development. As blockchain infrastructure matures and AI capabilities continue to advance, architectures of this kind may become increasingly feasible.

Overall, this study demonstrates that the convergence of AI and decentralized finance offers meaningful opportunities to improve efficiency, fairness, and usability in decentralized markets. By embedding intelligence into exchange architecture while preserving decentralization principles, future DEX platforms may evolve from passive execution venues into adaptive, user-centric financial systems. The design principles outlined here can serve as a reference point for ongoing research and development aimed at building more resilient and inclusive decentralized financial infrastructure.

References

- ◆ SoK: Decentralized Exchanges. (2021). "SoK: Decentralized Exchanges (DEX) with Automated Market Makers." *arXiv*. Available at: <https://arxiv.org/pdf/2103.12732>
- ◆ Bank for International Settlements (BIS). (2021). "Trading in the DeFi Era: Automated Market-Maker." *BIS Quarterly Review*. Available at: https://www.bis.org/publ/qtrpdf/r_qt2112v.htm
- ◆ BIS Working Paper No. 1227. (2024). "Decentralised Dealers? Examining Liquidity Provision in Decentralised Exchanges." Available at: <https://www.bis.org/publ/work1227.pdf>
- ◆ Blockstream. (2022). "Miner Extractable Value (MEV) and Programmable Money: The Good, The Bad, and The Ugly." Available at: <https://blog.blockstream.com/miner-extractable-value/>
- ◆ Chainlink. (2024). "Maximal Extractable Value (MEV)." Available at: <https://chain.link/education-hub/maximal-extractable-value-mev>
- ◆ Arkham Intelligence. (2025). "MEV: A 2025 Guide to Maximal Extractable Value in Crypto." Available at: <https://info.arkm.com/research/beginners-guide-to-mev>
- ◆ MDPI. (2022). "Promise of AI in DeFi: A Systematic Review." *Journal of Intelligence*, 2(1). Available at: <https://www.mdpi.com/2673-6470/2/1/6>
- ◆ On-chain Analysis Study. (2023). "A Comparative Study of Decentralized Exchange Activities on Ethereum, Solana, and Binance Smart Chain." *Business Accounting and Finance Research Journal*. Available at: <https://journal.wiseedu.co.id/index.php/bafrjournal/article/download/175/128/853>
- ◆ OSL. (2023). "How AI and Blockchain Are Shaping the Future of Decentralized Finance." Available at: <https://www.osl.com/hk-en/academy/article/how-ai-and-blockchain-are-shaping-the-future-of-decentralized-finance>
- ◆ OSL. (2023). "On-Chain vs. Off-Chain Cryptocurrency Transactions: What is the Difference?" Available at: <https://www.osl.com/hk-en/academy/article/on-chain-vs-off-chain-cryptocurrency-transactions-what-is-the-difference>
- ◆ Solana-focused AI Tokens Study. (2025). "AI-Based Crypto Tokens: The Illusion of Decentralized AI?" *arXiv*. Available at: <https://arxiv.org/html/2505.07828v1>

Table Sheet

Table 1: Comparison of On-Chain Trading Mechanisms

Feature	Traditional AMM (e.g., Uniswap V2)	Concentrated Liquidity AMM (e.g., Uniswap V3)	On-Chain CLOB (e.g., Serum)	Proposed AI driven Hybrid Model
Capital Efficiency	Low	High	High	Very High
Slippage Control	Poor for large trades	Good within range, poor outside	Very Good	Excellent (SOR-optimized)
Impermanent Loss Risk	High	Very High (for LPs)	N/A	Mitigated via Predictive MM
MEV Resistance	Very Low	Low	Moderate	High (with mitigation)
Gas Efficiency	Moderate	Low	High (on fast chains)	Moderate (hybrid cost)
Suitability for Agentic Trading	Low	Moderate	High	Very High

Table 2: Functional Roles of Agents in the Mult - Agent System

Agent	Role (Core Function)	AI Techniques	Primary Data Inputs	Primary On-Chain Actions
Smart Order Routing (SOR) Agent	Optimal trade execution and aggregation	Reinforcement Learning, Graph Algorithms	On-chain liquidity data (internal & external DEXs), Mempool data, Gas price feeds	Submitting optimized, potentially split, transactions to the settlement layer.
Predictive Market Making (PMM) Agent	Dynamic liquidity management and IL mitigation	Predictive Analytics (LSTM, Time-Series Forecasting), Sentiment Analysis	Historical price/volume data, Oracle price feeds, Social media/news feeds	Adjusting liquidity concentration ranges and fee tiers in the AMM via oracle calls.
Risk Management Agent	Real-time security and protocol health monitoring	Anomaly Detection, Formal Methods, ML-based Vulnerability Scanning	Transaction flows, Smart contract bytecode, Oracle price feeds, Collateralization levels	Triggering circuit breakers, pausing contracts, adjusting risk parameters (e.g., loan-to-value).
Governance Agent	Decision support for the DAO	Natural Language Processing (NLP), Economic Simulation, Game Theory	Governance proposals, Forum discussions, On- chain voting data	Submitting analysis reports to the DAO; simulating proposal impacts.

Table 3: Security Threats and Mitigation Strategies in the Proposed Architecture

Attack Vector	Description	Affected Component(s)	Architectural Mitigation Strategy
Re-entrancy	An attacker makes an external call to an untrusted contract, which then calls back into the original function before it has finished executing.	Smart Contract	Adherence to Checks-Effects-Interactions pattern; Use of re-entrancy guards; Formal verification of contract logic.
Oracle Price Manipulation	An attacker uses a flash loan to manipulate an asset's price on a source DEX, causing the oracle to report an incorrect price.	Oracle, Smart Contract, Risk Agent	Use of decentralized oracle network (DON); TWAP oracles for on-chain feeds; Cross-validation and circuit breakers managed by the Risk Management Agent.
AI Model Bias	The AI models make discriminatory or unfair decisions due to biased training data.	AI Agents (PMM, Risk)	Fairness audits; Use of diverse and representative training datasets; Continuous monitoring for performance disparities across demographic groups.
MEV Front-running	A searcher bot sees a user's transaction in the mempool and pays a higher gas fee to execute their own transaction first for profit.	On-Chain Layer (Mempool)	Integration with private transaction relays (e.g., Flashbots); Transaction batching to obscure individual order flow.
Governance Attack	A malicious actor acquires enough governance tokens to pass a proposal that drains protocol funds.	Governance Agent, DAO	Time-locks on governance proposal execution; Veto power for a security council; AI-driven simulation of proposal impacts to warn voters.

Empowering Agents, Transforming Markets: The Role of AI in Revolutionizing Life Insurance Distribution in India

UJJWAL RAJ¹

Students

BBA 2nd year (3rd semester)

RAJIV KUMAR MANGALAM²

Students

BBA 2nd year (3rd semester)

DR. TANMAY PANT³

Assistant Professor

SRMS International Business School,
Lucknow

Abstract

Artificial Intelligence (AI) has, over time, proved to be a game-changer for the Indian insurance industry with respect to empowerment of agents and the transformation of distribution channels. In customer interactions and scaling-up of operations, thus leading to improved decision-making capabilities of agents, AI is shaping the move from traditional customer representative (read, the agent) to those having AI-driven tools. With the incorporation of chatbots, predictive analytics, and automated underwriting, the current state of life insurance market is in stark contrast to what used to be a few years back all thanks to AI. These innovations have improved operational efficiency, personalization, and scalability although challenges in form of data privacy, digital literacy, and regulatory oversight do exist. Drawing upon a few cases studies from the life insurance space, this paper delves into describing the status-quo of an agent distribution that is AI-empowered and has been instrumental increasing their productivity, and is shaping the future of the insurance market.

Key Words: *AI; Agents; Predictive Underwriting; Personalization; Technology.*

Introduction

In sheer numbers, the Indian life insurance industry in terms of policies sold, is one of the largest yet, ironically, remains underpenetrated as compared to not only the advanced nations but also to some Asian peers. Cutting a sorry figure with respect to the life insurance penetration numbers as put forth by the Insurance Regulatory and Development Authority of India (IRDAI) at just 3.2% of GDP - far below the global average of 6.3% - the onus of enhancing these numbers lies with the distribution {most important P of the 7P's of Marketing and yet the weakest and the least explored in life insurance (Pant & Arya, 2019)}. While the distribution of life insurance is still agent-reliant with over 80% of policies being sold through this channel, other distribution channels have also come up.

While offering a personalised service and building trust, agents held sway for long and have been the mainstay of the Indian life insurance landscape. However, with the advent of the digital transformation and the breakneck speed at which technology (majorly AI) is redefining the rules of the game, the inherent weaknesses of the agent distribution (negating the gains to be had) have come to the fore: scalability, cost-efficiency, and response times of traditional agent-driven models are often limited, especially in rural and semi-urban areas where internet connectivity and digital literacy may be low. Initiatives like Digital India and

the subsequent adoption of digital services have revolutionized the way life insurance distribution is sold and the traditional agents have come in the firing line of this sweeping change.

For all the talk that the agents were bound to become a spent force and that their role would be limited in a distribution that is technology-intensive, AI's role in enhancing the capabilities of the agents, in addition to giving them a wider reach, has put to rest some of the weaknesses of the agent-distribution set up. For streamlining the customer journey, smoothening the operational efficiency, and increasing the outreach all thanks to automated underwriting, predictive analytics, AI-powered chatbots, and lead scoring, insurers are utilizing these tools in a manner that has radically transformed the distribution dynamics.

While discussing the broader market changes brought about in wake of AI interventions, this paper will remain fixated to the all-important agent distribution that has been the driver of life insurance sales in India and has been in the spotlight in these technology-advanced times dictated by the role of AI. Towards that end, the paper will discuss how AI is helping agents enhance their productivity, engagement, and customer trust, as also improving customer experience, and influencing the overall structure of the market. IRDAI based data and cases of HDFC Life and ICICI Prudential are

central to the findings of this study that attempts to comprehend the clarity around AI's influence on the traditional agents.

Literature Review

At a time when AI is redefining value chains across industries and sectors, the global life insurance industry and along with it, the Indian counterpart is actively engaging with this shift. This literature review explores relevant studies, industry inputs, and few cases to fully comprehend the transformation brought about by the AI phenomenon in the distribution space.

Traditional Distribution Channels in Indian Life Insurance

IRDAI's Annual Report 2022-23 provides the context in which agent-based distribution comprising of over 2.5 million agents accounts for over 80% of life insurance sales (IRDAI, 2023). Performing multitude of tasks from educating buyers in rural and semi-urban areas to policy simplification and building trust through personal rapport, these agents, especially those from the Life Insurance Corporation of India (LIC) – the state-run giant that accounts for majorly all the policy sales in the industry through agents – handle majority of new business premiums (Lakhangaonkar et al., 2022).

This model, however, suffers from structural inefficiencies:

- High customer acquisition costs, often exceeding 20-30% of premiums in the first year.
- Long onboarding cycles, sometimes taking weeks due to manual paperwork.
- Limited scalability beyond regional geographies, particularly in underserved areas.

Even bancassurance, while growing to account for about 15-20% of distribution, has struggled to break out of urban centers due to limited financial inclusion in tier-3 regions (IBEF, 2024). These drawbacks have paved the way for AI and digital tools that offer automation, speed, and cost efficiency (Bharti AXA, 2024; Maheswari, 2025).

Global and Indian Trends in AI-Driven Distribution

Globally, AI is being leveraged to achieve the dual benefits of cost optimization and customer-centricity. McKinsey & Company (2022) report that a whopping 20% increase in

conversion rates along with 30-50% reduction time in onboarding and claims could be attributed to AI-enabled systems in place. Specifically, new-agent success rates and sales conversions through AI transformations in sales and distribution have gone up 10-20% in case of the best insurers of the world (McKinsey, 2025). For example, AI-powered chatbots and predictive models have enhanced customer satisfaction by 36% after enabling 80% of transactions to move online,.

In India, this digital acceleration is due to:

- Initiatives of the government that have enabled faster customer onboarding. Digital India and Aadhar e-KYC are few such initiatives undertaken.
- Connectivity enhancement as a result of increased internet penetration and an upsurge in the smartphone and mobile usage with over 800 million users providing the necessary impetus.
- Technologies such as IoT for telematics-based risk assessment and RPA for back-office automation (IBEF, 2024).

Examples from India include:

- HDFC Life's chatbot "Elle" guides users through premium estimates, document upload, and policy comparison, reducing administrative burdens.
- ICICI Prudential's "LiGo" acts as a virtual sales assistant that answers customer queries instantly, reducing agent workload and improving lead conversion (Maheswari, 2025).
- Digit Insurance uses AI for end-to-end digital sales, with real-time risk profiling and paperless onboarding.
- Video-based KYC and optical character recognition is extensively used by firms like SBI Life by leveraging AI, in turn, reducing staff dependency and enhancing efficiency (Lakhangaonkar et al., 2022).

Estimated to reach US\$ 222 billion by 2026, the Indian insurance market is primed to incorporate RPA and AI in its processes and that is already reflected through better data processing and advancements in algorithms for personalized services (IBEF, 2024).

An increase in AI applications between 2018-2023 is reflected through empirical data obtained from insurers like Acko and Shriram which automate claims and use ML for fraud detection (Maheswari, 2025).

AI-Augmented vs. AI-Driven Models

Researchers and practitioners have drawn a useful distinction between AI-augmented and AI-driven distribution:

- **AI-Augmented Models** integrate AI tools into human-led processes. Agents use AI for lead prioritization, customer education via digital platforms, and CRM automation. Companies like LIC and Max Life follow this hybrid approach. For instance, Max Life agents use a mobile app that leverages AI to suggest the best policies based on the client's age, income, and health profile, while also employing NLP for sales support and AI-based campaign engines like Suraksha (Lakhangaonkar et al., 2022). Kotak Life Insurance uses assistive bots and voice AI like KAYA for instant policy information, serving 53% more customers efficiently.
- **AI-Driven Models** automate the entire customer journey. Digital-first firms like Acko and Turtlemint allow customers to purchase insurance without human intervention. Their platforms feature dynamic pricing, instant issuance, and AI-powered chat support, with examples like Tata AIA using AI for real-time fraud detection in underwriting (Maheswari, 2025).

As much as the delineation regarding the above typology is useful, it is to be kept in mind that the pace and nature of AI adoption varies by companies and augmented models dominate traditional insurers and driven models dominate insurtechs (McKinsey, 2025).

Enhancing Reach and Financial Inclusion through AI

Since AI has donned many hats, one of its other roles is transforming the improvement related to enhancing access to insurance for underserved markets, particularly in rural and low-income segments, much in-sync with "Insurance for All by 2047" vision of the IRDAI. (Maheswari, 2025).

Key AI enablers for inclusion, include:

- **Vernacular AI chatbots:** Platforms like Gram Cover and Policybazaar are developing tools that support regional languages and voice-based input, with Niva Bupa's "CIA" resolving millions of queries in multiple languages.
- **Speech-to-text and low-bandwidth solutions:** Critical for areas with weak internet access or low literacy, as seen in BIMA's mobile onboarding with biometric verification.
- **Micro-insurance pricing:** AI analyzes income and demographic data to tailor ultra-low premium products, reducing fraud and expanding coverage (IBEF, 2024).

For example, BIMA, a rural India based firm uses AI

through mobiles to onboard users, taking paperwork out of the equation in the process. The protection gap is reduced drastically through Insurtech partnerships thus helping scalable delivery systems to close the protection gap (Munich Re, 2024).

AI in Consumer Experience and Decision-Making

Research has shown that AI improves the speed, customer engagement, and personalization and the same is reflected through the research by Deloitte India (2022) that shows that hyper-personalised digital journeys shoots up engagement rates by 30-40% in financial services.

Capabilities include:

- **Predictive underwriting:** making an assessment of risk and health profiles using historical and behavioural data, a case in point being HDFC Life using machine learning for risk mitigation and customer retention (Lakhangaonkar et al., 2022).
- **AI-generated advice:** Advice at each stage of life, income, and aspirations much like in ICICI Prudential's nudge engines does a world of good for potential consumers.
- **24/7 availability:** AI-powered chatbots bring down the turnaround time much like Aviva's AI models cutting liability assessment by 23 days (McKinsey, 2025).

In spite of the above capabilities, consumers tend to have more faith in AI when there is a human capability to fall back upon. As the insurance gets complex, emotional assurance especially during claims and disputes takes centre stage and hence it calls for human fallback even when AI is used.

Regulatory, Ethical, and Operational Challenges

Despite the upside, AI integration in life insurance distribution faces real constraints in India.

- **Data Privacy:** Lack of standard protocols on personal data collection and analysis warrants a fully operational Personal Data Protection Act as its absence is linked with risks of misuse and cyberthreats (Swiss Re, 2023). As AI relies heavily on data, challenges regarding data privacy continue to exist.
- **Digital Literacy:** Lack of skills regarding specific AI related features especially in rural areas make AI integration a big challenge (IBEF, 2024).
- **Algorithmic Bias:** AI can unintentionally discriminate if trained on flawed datasets—impacting premium pricing

or claim rejections, as warned in sonar reports on AI risks (Swiss Re, 2024).

- **Agent Resistance:** Traditional agents resist the AI digital change more so when they see it as a potential challenge for their jobs unless trained on co-creation (Maheswari, 2025).
- **Evolving Risks:** Swiss Re (2024) emphasizes upon continuous adaptation due to AI's dynamic nature with potential for "silent cyber" exposures in underwriting biases leading to lawsuits.

Swiss Re (2023), as a downside of incorporating AI, states that without ethical AI governance, extant systems, even unintentionally, may widen the trust gaps and access. Strategies for trust-building and maintenance of human oversight should be in place in view of the rapid evolution from rule-based to machine learning and generative AI (Swiss Re, 2024).

Case Studies and Examples

1. HDFC Life – AI-Powered Virtual Assistant “Elle”

Background: HDFC Life has unleashed an AI-driven virtual assistant named Elle to support the personalised service delivery of agents. It helps the agents to fact-find customer's requirements, generate quotes, suggest suitable products matching customer profiles, and even manage claims.

Impact: This AI tool has been instrumental in reducing agent time on administrative tasks allowing for focus on building customer relationships and closing sales.

Agent Empowerment: Elle has empowered agents through augmentation of their digital skills and giving more time to interact with customers. Elle has got great customer feedback on account of streamlined policy recommendations and claim processing.

2. ICICI Prudential – AI-Powered “LiGo”

Background: ICICI Prudential has developed the LiGo platform with a chatbot that is meant to serve the customers and agents. It navigates the agents to identify value-creating leads and real-time customer data while offering tailored policy suggestions to customers.

Impact: The AI-powered chatbot has led to faster policy issuance and effective lead conversion. Agents have gone on record stating that higher sales conversions have been made possible due to predictive analytics and lead scoring and this has further helped prioritise interactions.

Agent Empowerment: Freeing up agents' time by automating lead management and customer interactions, LiGo allows agents to focus on high-value tasks like relationship-building and finalizing sales.

Limitations of the Study

Notwithstanding the vital insights gained about AI's role in transforming life insurance distribution and empowering agents in India, this study, like others, is plagued by limitations that accompany both the methodology and scope of the study.

Scope and Generalizability

While life insurance sector specific agent empowerment at the back of AI-capabilities has been covered in detail in this paper, it does leave out scope in the other insurance segments viz. Health and General Insurance. Henceforth, the findings are not generalised for the insurance industry. Similarly, the study has litter to offer for other countries where regulatory, technological, and cultural contexts differ. Additionally, the selected case studies of HDFC Life and ICICI Prudential provide depth but do not represent the diversity of technological maturity across all life insurance providers in India, especially smaller ones or ones that are rural-focused.

Rapid Technological Change

AI's proliferation and growth is rapid meaning thereby that the paper might not provide an accurate snapshot of the current trends in AI in augmenting the agent force. The findings may require constant updation on account of the fast-evolving ecosystem that has the potential to render the current status-quo redundant.

Regulatory and Policy Uncertainty

In its partial avatar, the Personal Data Protection Act has not yet established firm AI governance frameworks. Still under formulation, India's data protection and digital infrastructure policies do not translate into direct policy formulation. The research thus navigates a degree of legal and compliance ambiguity that may shift in the near future.

Conclusion

Artificial intelligence is changing the future of distribution in life insurance in India. AI is enhancing the life insurance

agent's role in a positive way by augmenting the life insurance agent's expertise. In addition to improving the operational efficiency of agents, AI is elevating customer engagement, personalization, and increasing access to insurance where it has been lacking in low and underserved rural and semi-urban markets. Use case examples, such as HDFC Life's Elle and ICICI Prudential's LiGo illustrate how AI provides agents with assistance in supporting their appropriate traditional agent role through automating all routine tasks, providing agent with data to enhance standard practice, and utilizing agent's time better by spending more of it on forming relationships and high-value activities.

While increased performance through agent utilization of AI advances the role agents play in life insurance, new operational challenges will arise with the deployment of AI - such as data privacy, digital literacy, algorithmic bias, and regulatory oversight. In promoting trust and optimizing the benefits of innovations driven by AI, we need to address challenges through ethical AI governance, stakeholder training, and agent facilitative regulatory policies.

As a whole, AI is not replacing agents but changing the role agents play in life insurance so they have more productive, informed, and customer centered approaches to the distribution of life insurance. The Indian life insurance market is moving towards a more collaborative model, whereby AI and Agents support each other, for better penetration rates, on going financial inclusion, and a more innovative, efficient insurance market.

References

- ◆ Bharti AXA. (2024). *Life Insurance Plans and Digital Transformation*. Bharti AXA Life Insurance Company. Retrieved from <https://www.bharti.axa.com/>
- ◆ Deloitte India. (2022). *Hyper-Personalized Digital Journeys in Financial Services*. Deloitte Touche Tohmatsu India LLP.
- ◆ IBEF. (2024). *Growth of the Indian Insurance Industry with Market Size & Trends*. India Brand Equity Foundation. Retrieved from <https://ibef.org/industry/insurance-sector-india>
- ◆ IRDAI. (2023). *Annual Report 2022-23*. Insurance Regulatory and Development Authority of India. Retrieved from <https://irdai.gov.in/annual-reports>
- ◆ Lakhangaonkar, S., Ubale, D., & Ubale, S. (2022). *Artificial Intelligence Applications in the Life Insurance Sector: A Study of Select Life Insurance Companies in India*. ResearchGate. <https://doi.org/10.13140/RG.2.2.12345.67890>
- ◆ Maheswari, V. U. (2025). *Application of Artificial Intelligence and Machine Learning in the Indian Insurance Industry*. ResearchGate. <https://doi.org/10.13140/RG.2.2.98765.43210>
- ◆ McKinsey & Company. (2022). *AI-Enabled Insurers: Cost Optimization and Customer-Centricity*. McKinsey & Company.
- ◆ McKinsey & Company. (2025). *The Future of AI in the Insurance Industry*. McKinsey & Company. Retrieved from <https://www.mckinsey.com/industries/financial-services/our-insights/the-future-of-ai-in-the-insurance-industry>
- ◆ Munich Re. (2024). *Insurtech's Role in India's Race Towards 'Insurance for All' by 2047*. Munich Re. Retrieved from <https://www.munichre.com/automation-solutions/en/resources/blog/insurtech-s-role-in-india-s-race-towards--insurance-for-all--by-.html>
- ◆ Pant, T., & Arya, S. (2019). *Distribution problems in private bank led life insurance firms: a contrasting scenario in the Indian context*. *International Journal of Engineering and Advanced Technology*, 8(5s3), 317-326.
- ◆ Swiss Re. (2023). *Ethical AI Governance in Insurance*. Swiss Re Institute.
- ◆ Swiss Re. (2024). *The Evolution of AI in the Insurance Industry*. Swiss Re. Retrieved from <https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/evolution-of-ai-in-insurance-industry.html>

The Implication of AI in the Business: Skills, Experiences, and Future Development in the Time of Uncertainty

ANKITA AGARWAL¹
eng.ankita.agarwal@gmail.com

SOVAN MOHANTY²
mohanty.sovan@gmail.com

MAHENDRA SINGH³
mahendra.singh@srmscet.edu

SRMS College of Engineering & Technology,
Bareilly, India

Abstract

This paper provides a close examination of what has been said regarding the impact of artificial intelligence (AI) on the growth of businesses. With the process of artificial intelligence (AI) changing the nature of industries, the role of this process in organizational development, employee capacity, and customer relations can become crucial to comprehend. I desired to draw together a decent collection of the shaken fields of business development by AI, the benefits, and the obstacles that it presents. AI allows companies to do menial tasks automatically. Such things as machine learning, chat-based AI, and automated systems have the potential to transform the industries completely by identifying trends before they occur, tailor what customers receive, and smarter resource utilization. However, it does not go that way without issues, companies are forced to address concerns about data security, hacks and ensuring that algorithms do not discriminate a group of people. Based on the qualitative analysis and combined knowledge, we present three possible futures: the steady integration, the rapid rollout, and the targeted implementation. The results indicate that, although AI can enhance efficiency and innovation, adaptive training and ethical protection are also required. This paper will provide evidence-based advice to leaders who want to handle AI-based change and focus on balanced approaches to achieve sustainable development.

Key Words: *Artificial intelligence, return on investment, scenario planning, ethical integration, foresight strategies.*

Introduction

Artificial intelligence is a game-changer in the current world that is a fast-paced environment where companies are present worldwide. It is no longer simply about automation of the tasks but AI is pushing the frontiers in the way the firms conduct business, relate with the customers and strategizing on the future. Consider how such products as predictive algorithms or smart assistants are already entering the markets in such industries as manufacturing or hospitality. However, along with all this possibility, there is uncertainty, what should AI destroy work more than it should generate it? Or how are companies supposed to make sure it is being used to benefit experiences and not to kill people?

The paper begins to explore these questions by examining how AI has more general implications of growth, skills, and interactions. We are basing our project on existing studies that take a proactive approach to strategize the possibilities, but not merely respond to the current trends. As an example, an early adopter of AI has been reported to experience productivity leaps up to 40 percent, depending on the reports conducted by McKinsey Global Institute (Manioca et al., 2017). However, the difficulty is in being ready to have mixed results. In this instance we would apply scenario planning, a technique that has been tested to work well in the

uncertain context, to draw out the direction of the future. Our goal? To make managers develop the strategies that would transform AI into meaningfulness into the actual source of success.

I. Literature Review

As labor increases then the transformative power of AI in business environments. Originally they concentrate on the technical aspect of the matter such as how machine learning could move through information to identify trends that human beings could overlook. The more recent discourse is framed in terms of the human factor: how AI is changing what employees have to know and do. Indicatively, studies indicate that as AI performs more menial tasks, employees have to upgrade in other areas such as problem-solving and collaboration skills, which are not in competition with technology.

According to the expertise of customer experiences especially in dynamic environments such as events, AI is perceived to be a point of contact to more personalised experiences. Interactions can be personalized with the help of chatbots or recommendation systems, which will make the participants feel appreciated and increase satisfaction. Nevertheless, it is not as simple; excessive involvement of

AI could eliminate the human factor that makes the events memorable (Ivanov and Webster, 2017). Research on service sectors indicates that with appropriate integration of AI, it can enhance value generation, in which customers and providers jointly construct experiences using common assets.

It is proved that AI is growing in terms of optimization of activities and new markets. An example of how AI-powered analytics are applied to small firms is predicting demand to reduce waste and expand more quickly. However, there are still issues, such as the threat of data security and the necessity of moral codes to prevent algorithmic bias. More general reviews have shown that organizations that have developed powerful AI strategies tend to perform better than their counterparts with some reporting a 15-20% increase in revenue. However, this relies on aligning AI with their overall objectives, making investments in training, and managing likely negative effects such as staff displacement.

Three threads - skills, experiences and growth these threads are linked together at varying rates of adoption of AI. This review summarizes findings to suggest proactive planning where businesses foresee changes instead of rushing to keep up.

To make the maximum of AI to develop, one needs to be smart. Organizations are supposed to align AI activities with their overall objectives and develop comprehensive implementation strategies. Brynjolfsson and Hutt (2018) and Ross et al. (2019) emphasize the importance of checking tech setups, training to fill gaps in skills, and establishing moral rules. With a good fit, AI fits seamlessly into processes to continue development.

AI also leads to innovative thoughts in other areas. It may result in new products, services or entire business modes. Teece (2018) and Bughin (2019) demonstrate how AI can take things to the limit by automating difficult work and uncovering information secrets. Adopting this is capable of differentiating firms and enhancing development.

II. AIMS

- See the impact of AI on business growth: This examines the impacts on decisions, forecasts, marketing, risk and customer support.

- Win or lose in applying AI: Learn about advantages such as making better choices, creating personalized experiences, using resources more intelligently, and ethics and issues.
- Get the impacts of AI on diverse disciplines: Explore how it has been struck finance, health, making stuff, retail-sharing cases, pros, cons in related areas.
- Propose how to implement AI successfully: Based on the findings of the review, provide recommendations on how to work with data, find the right talent, train, address ethics, fix risks. Concisely, this contributes to the familiarization with the role of AI growth and provides useful guidance towards intelligent, justifiable use.

III. Methodology

In an attempt to peer into the future implications of AI, we used a scenario method, which is a qualitative approach best suited to the answer to questions of the form, what if. This technique, which is present in studies about foresight, is creating plausible storylines through existing trends and professional contributions. We began by examining such critical drivers as technological advances, regulatory, and market needs and developed three scenarios reflecting different AI adoption speeds: gradual (slow and steady), aggressive (full-speed ahead), and selective (focused on high-impact areas).

In each case, we performed SWOT analysis (evaluating our strengths (internal positives), weaknesses (internal limitations), opportunities (external potentials), and threats (external risks). This assisted in finding strategic responses. The data was obtained by synthesis of the given documents, I added statistical touches as a statistician, estimating probabilities using surveys of the industry, such as a 60% chance of gradual adoption in stable industries such as finance, which I found in a report of Deloitte on AI trends in 2024.

To guarantee durability, we cross-validated scenarios against real-world cases, e.g. AI in event planning based on case studies. Our practice was informed by the ethical considerations, without biased assumptions and centered on the inclusive results.

IV. Results

In our analysis, we have identified three different futures of AI in the business with different implications of growth, skills, and experiences.

In Scenario 1: Gradual Integration, a gradual merging of contemporary technologies and software across workplaces is observed. In Scenario 1: Gradual Integration, contemporary technologies and software are merged in workplaces gradually. In this direction, AI is introduced gradually, which means it has time to adapt. Advantages are little disturbance and gradual skills development, such as progressive data literacy training and the weaknesses are possible competitiveness in case competitors go faster. The possibilities of collaborative human-AI teams increase productivity by 25-30 percent, according to some estimates (Accenture, 2022). Regulatory delays that halt innovations are some of the threats.

In the case of workforce skills, employees acquire hybrid skills over time, i.e. technical knowledge and creativity. At event level AI may process logistics such as scheduling, freeing up human beings to meaningful interactions, with a small growth of 10-15% efficiency.

In Scenario 2 : Smoother Rollout incurred greater expenses and did not achieve the intended outcomes because it moved too swiftly in its implementation. Scenario 2: Aggressive Rollout. In Scenario 2, Smoother Rollout incurred more costs and failed to realize the desired results due to its speedy implementation.

Here, firms plunge directly into the deep water, implementing AI through its operations. Strengths: Quick improvements in automation, which can even increase the production of certain fields such as supply chains. High costs and a lack of cooperation among employees who are afraid to lose their jobs can be listed as weaknesses-according to surveys 40% of employees have concerns about this (Pew Research Center, 2023).

Opportunities: The explosion of the business by innovations such as AI-enhanced personalization, increasing the recognition of customers by up to 35. Risks: Threats of ethical risks like data breaches would destroy trust. Skills radically change to the more sophisticated, analytic and monitoring and the event experiences are hyper-personalized, creating a viral impact, but creating potential overload.

In Scenario 3: Selective Implementation. Competitive Advantages Cost-effective and low-risk Simple wins in focused growth Strengths Strengths: Cost-effective and low-risk with quick wins in focused growth. Weaknesses:

Scaling required collaborating. Opportunities: Niche leadership, i.e. AI-enhanced events lead to 20 percent higher satisfaction levels (Event MB, 2024). Scenario Key Growth Impact: Skills Shift Necessary Experience Enhancement Probability Estimate.

Bit by Bit Consistent 10-15% increase Data literacy + cooperation Basic personalization 60 percent. Aggressive Rapid 25-40% increment Fast-tracked analytics and management Hyper-customized interactions 25%. Discriminatory 15-25% profitability Targeted ethics + tech integration Focused enhancements 15%. These are based on industry aggregate data, and with gradual being the most likely in risk-averse markets.

V. Discussion

The scenarios highlight the duality of AI to drive forward as long as it is managed in a responsible manner but a step toward failure when it is not, since the most relevant cases to the business (such as AI training programs in Google) demonstrate the breadth of deskilling. To grow, integrating in line with core values is the secret, which may not fall into the pit of technology to technology.

Artificial intelligence has the potential to turn active co-creation into passive attendance in the context of events; however, it requires human elements to be enhanced. Ethical questions seem giant; lack of transparency may expand disparity of AI. To develop strong teams, leaders ought to encourage cultures of lifelong learning and this would be done in collaboration with teachers. Limitations: Scenarios are theoretical, albeit based on data. Research in the future may be able to quantify the effects using longitudinal research.

Conclusion

AI is not a tool, but it is a force that is transforming the landscape of business development, employee adaptation, and experiences. What our situations demonstrate is that success is reliant upon strategic choices: be it gradual to achieve stability, be it aggressive to make bold leaps, or be selective to achieve precision. Some of the suggestions made are to audit existing capabilities, invest in ethics-based training, and observe tendencies to rotate when necessary. Organisations can use the present moment to overcome any AI uncertainties to become sources of sustainable progress.

References

- ◆ Bobitan N, Dumitrescu D, Popa AF, Sahlian DN, Turlea IC (2024, January). Shaping tomorrow : Anticipating skills requirement based on the integration of Artificial Intelligence in business organisation- A foresight analysis using the scenario method (2024), *Electronics* ; 13 (11) :2198.<https://www.mdpi.com/2079-9292/13/11/2198>.
- ◆ Hansen, E. B., & Bøgh, S. (2021, January). Artificial intelligence and internet of things in small and medium-sized enterprises: A survey. *Journal of Manufacturing Systems* , 58 , 362 – 372 . <https://doi.org/10.1016/j.jmsy.2020.08.009>
- ◆ Rudab SA. (2023, August). Impact of AI on business growth. *The business management review*, 14(02). https://cberuk.com/cdn/conference_proceedings/2023-13-16-29-12-PM.pdf.
- ◆ Pew Research Center. (2023). AI and Jobs Survey. Pew Reports.
- ◆ World Economic Forum. (2023). The Future of Jobs Report 2023. WEF Publications
- ◆ Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age*. W.W. Norton & Company.

Artificial Intelligence in Human Resource Management : A Review of Application in Employee Engagement and Performance Evaluation

MR. AMAAN KHAN¹
amaankhan88719@gmail.com
Corresponding Author
Student-MBA, SRMS IBS, Lucknow

MS. INSHA FATIMA²
inshi23fatima@gmail.com
Student-MBA, SRMS IBS, Lucknow

MS. SURBHI MISHRA³
mishrasurbhi892@gmail.com
Student-MBA, SRMS IBS, Lucknow

MS. SAMAN ASHRAFI⁴
saman.ibs@srms.ac.in
Assistant Professor
Departmental of Management
SRMS IBS, Lucknow

Key Words: *Artificial Intelligence, Employee Engagement, Performance Management, HR Analytics, Organizational Development, Human Resource Management (HRM), Talent Retention.*

Abstract

In the swiftly changing digital work environment of today, companies are progressively utilizing Artificial Intelligence (AI) to revolutionize conventional Human Resource Management methods. This study investigates the incorporation of AI tools in improving employee involvement and performance assessment. The research investigates how AI-based tools—like sentiment analysis, predictive analytics, chatbots, and tailored feedback systems—can deliver immediate insights into employee behavior, motivation, and productivity. Through the automation of repetitive tasks and the facilitation of data-driven decision-making, AI creates a more adaptive and tailored workplace, leading to enhanced employee satisfaction and better organizational performance. The document examines possible ethical issues, data privacy matters, and the significance of upholding a human-focused approach in AI applications. This research emphasizes best practices and presents a strategic framework for effectively leveraging AI to enhance employee engagement and performance outcomes through case studies and an assessment of existing AI applications

Potential difficulties like algorithmic transparency, data privacy, and ethical issues in workforce analytics are also covered. The results demonstrate that, in the age of digital transformation, AI-enabled engagement and performance platforms support ongoing learning and organizational expansion in addition to increasing productivity and retention.

Introduction

In a time of growing competition and digital transformation, businesses are always looking for new and creative ways to improve employee happiness and productivity. Employee engagement and performance management, two elements that have a major impact on organizational success, employee retention, and general workplace morale, are among the most important components of human resource management (HRM). Periodic surveys, manual performance reviews, and subjective evaluations are frequently used in traditional methods of managing performance and engagement. These approaches can be reactive, time-consuming, and inconsistent.

Organizational approaches to employee engagement and performance are changing as a result of the tremendous new capabilities brought about by the development of artificial intelligence (AI). From machine learning and intelligent automation to predictive analytics and natural language processing, artificial intelligence (AI) technologies present previously unheard-of chances to collect data in real-time, spot trends, and provide individualized insights at scale. With the use of these tools, managers and HR specialists may better understand the needs of their workforce, handle possible problems before they become serious, and encourage ongoing performance enhancement.

In addition to discussing important ethical issues like data privacy, algorithmic bias, and the need to maintain human empathy in AI-driven processes, this paper explores how AI can be successfully incorporated into employee engagement and performance management systems. It also looks at the tools and technologies

currently in use, their effects on workplace dynamics, and the potential advantages and difficulties of implementing AI in HR practices. By analyzing current trends, case studies, and empirical findings, this research attempts to provide a thorough understanding of how AI can act as a strategic enabler for creating workforces that are more engaged, productive, and prepared for the future.

However, incorporating AI into performance management and employee engagement also brings up a number of operational and ethical issues, including data protection, algorithmic decision-making transparency, and the possibility of bias in automated assessments. Thus, it is essential to comprehend how AI might be applied to HR procedures in a way that is both efficient and moral. The purpose of this research study is to examine how AI can be used to modernize performance management and employee

engagement procedures while evaluating its advantages, drawbacks, and potential future effects on workforce development sustainability.

This research explores how Artificial Intelligence (AI) is transforming employee engagement and performance management in modern organizations. By leveraging machine learning, predictive analytics, and natural language processing, AI-driven systems can identify employee sentiment, personalize engagement strategies, and offer real-time performance feedback. The study examines how AI enhances decision-making for HR professionals by reducing bias, improving objectivity in performance evaluations, and fostering a data-driven work culture. It also discusses potential challenges such as data privacy, algorithmic transparency, and ethical considerations in workforce analytics. The findings highlight that AI-enabled engagement and performance platforms not only improve productivity and retention but also contribute to continuous learning and organizational growth in the era of digital transformation.

Through the introduction of new capabilities for data-driven decision-making, personalization, and proactive HR interventions, artificial intelligence is transforming performance management and employee engagement. Real-time feedback, personalized learning and development, and the ability to anticipate engagement or performance risks before they become issues are all made possible by AI-powered platforms. By automating time-consuming HR duties like leave administration, attendance tracking, and feedback cycles, these solutions enable managers to concentrate on strategic work and improve employee relations.

Objective

- To examine the role of Artificial Intelligence in Human Resource Management
- To review AI applications that enhance employee engagement and performance evaluation
- To identify the benefits and challenges of using AI in HR processes.
- To analyze recent trends and research findings related to AI-driven HR practices
- To provide recommendations for effective and ethical use of AI In Human Resources Management

Literature review

The use of Artificial Intelligence (AI) in Human Resource Management (HRM) is commonly talked about in recent studies as a trend that is sure to happen and changes how things are normally done. Because of the need for digital change, AI is seen as a key technology that affects many areas of business. In managing people, the main goals of using AI are to make performance management more efficient and to keep employees engaged over time. Experts say AI helps make decisions based on data, lowers bias, and lets companies focus more on the human parts of managing people. Theoretical Underpinnings and Frameworks for Acceptance

A few well-known theories often serve as the foundation for academic research on the use of AI to human resource management.

The addition of AI to performance management systems to improve their functionality is explained by systems theory.

Employee attitudes on the employment of AI tools are frequently examined using the Technology Acceptance Model (TAM).

According to studies, people are more likely to accept AI if they believe it would be beneficial, such as improving insights or increasing productivity. However, it's crucial to consider how unsafe people perceive AI when employing it for critical activities like performance reviews.

Through the introduction of data-driven methods for performance management and employee engagement, artificial intelligence (AI) is revolutionizing human resource management. According to recent research, AI-powered solutions like chatbots, predictive analytics, and performance dashboards assist businesses in tailoring communications, spotting disengaged workers early, and offering ongoing feedback.

But researchers also highlight possible disadvantages. Over-reliance on AI may result in algorithmic bias, privacy issues, and less human connection, all of which could have a detrimental impact on morale and trust (Kaur & Sharma, 2022). The organization's preparedness for digital transformation, ethical governance, and employee acceptance all play a major role in the success of AI applications. Therefore, it is essential to combine human judgment with AI insights in order to preserve fairness and empathy in decision-making.

Overall, research shows that although AI greatly improves productivity and objectivity in managing worker engagement and performance, it must be used responsibly. Future studies should concentrate on ethical issues, long-term effects, and striking a balance between automation and human interaction.

But problems still exist. Algorithmic bias can be inherited by AI systems from training data, and sensitive data collecting poses serious privacy issues that necessitate adherence to laws like GDPR. Close AI surveillance can psychologically cause stress and a loss of autonomy unless the technology is openly presented as a tool for growth rather than a harsh assessment. Therefore, Explainable AI (XAI) and a hybrid model that strikes a balance between algorithmic efficiency and crucial human

judgment and ethical governance are essential for successful adoption.

However, there are still challenges. AI systems can pick up biased patterns from the data they're trained on, and gathering personal information brings up big privacy issues that need to follow rules like GDPR. On the mental side, being watched too closely by AI can cause stress and make people feel like they're losing control, unless the technology is clearly seen as helping them grow instead of judging them. For AI to be used well, it needs to be explainable so people understand how it works. Also, a mix of smart algorithms and human judgment, along with strong ethical rules, is key to making it work properly.

But the literature also alerts readers to a number of difficulties. An excessive reliance on AI could diminish the human component of management, raising issues with data security, privacy, and fairness. If left uncontrolled, bias in AI systems can exacerbate already-existing disparities in the workplace. Researchers like Gupta (2024) stress that companies using AI-driven HR procedures need to maintain human control, develop ethical standards, and guarantee transparency.

In conclusion, even if AI has enormous potential to improve performance management and employee engagement, its success hinges on its appropriate use, employee trust, and compatibility with company culture. The long-term effects of integrating AI, ethical governance, and striking a balance

between machine intelligence and human intuition in workforce management should all be investigated in future studies.

An "inevitable development trend" that radically changes employee engagement (EE) and performance management

(PM) is the use of artificial intelligence (AI) into human resource management (HRM). The literature emphasizes AI's role in transitioning from static annual assessments to continuous, data-driven systems, based on models such as the Technology Acceptance Model and Conservation of Resources theory.

Research Methodology

Research Design: This study adopts a qualitative and descriptive research design based on a comprehensive review of secondary data. The aim is to explore and synthesize existing literature, reports, and case studies that examine the applications of Artificial Intelligence (AI) in Human Resource Management (HRM), with a specific focus on employee engagement and performance evaluation.

Data Collection Method

The research relies solely on secondary data sources. These include:

- Peer-reviewed journal articles
- Conference proceedings
- Industry papers and reports (e.g., from McKinsey, Deloitte, PwC, Gartner)
- Books and book chapters related to HRM and AI
- Reputable online databases and academic repositories such as:
 1. Google Scholar
 2. Scopus
 3. Web of Science
 4. JSTOR
 5. ScienceDirect

The data collected spans publications from 2020 to 2025, capturing the evolution of AI applications in HRM over the last decade.

Data Analysis Method: The collected literature was analyzed as follows:

1. Reading and grouping the data to identify key concepts

and findings.

2. Synthesizing insights across different sources to highlight patterns, trends, benefits, challenges, and gaps in current applications.

Findings

- **Positive Correlation between Engagement and Performance:** The study discovered a significant positive correlation between the outcomes of performance evaluations and employee engagement. Stronger commitment, increased productivity, and improved alignment with company objectives are all characteristics of highly engaged workers.
- **Impact of Recognition and Feedback:** Frequent performance evaluations and acknowledgment have been identified as key factors influencing engagement. Workers were more driven to develop and perform better when they received positive comments and recognition for their efforts.
- **Management and Leadership's Role:** Engagement and performance results are greatly impacted by leadership style. Employee trust and a sense of belonging are increased by supportive and participative management techniques, and this improves performance reviews.
- **Influence of Work Environment:** When the workplace is positive and welcoming, people are more involved and motivated. Workers in places where communication is clear, teamwork is encouraged, and there's openness to meet their

goals more consistently. Also, offering training and opportunities for career growth is important for employee development.

Interpretations

- Performance and productivity are directly impacted by employee engagement.
- An efficient performance review increases employee growth and motivation.
- Fair criticism and acknowledgment boost confidence and contentment at work.

- Engagement levels are raised by effective leadership and honest communication.
- Evaluation is more precise and customized when AI is used.
- Performance evaluation and engagement are interdependent.
- Higher productivity and organizational success are fueled by engaged workers.

Research Gap

- **Limited AI Integration in Engagement Research:** The majority of earlier research has concentrated on conventional approaches to employee engagement, with little attention paid to the application of artificial intelligence (AI) in performance assessment and engagement enhancement.
- **Insufficient Industry-Specific Research:** Research comparing engagement and performance evaluation methods across several industries, including the IT, healthcare, and education sectors, is scarce.
- **Insufficient Attention to Psychological and Emotional Aspects:** Numerous studies focus on productivity results while ignoring employees' psychological engagement and emotional health.
- **Insufficient Data on Remote and Hybrid Work Settings:** Post-pandemic work models have changed engagement dynamics, yet research on how remote or hybrid work affects engagement and performance evaluation is still scarce.
- **Gap Between Evaluation and Action:** Although organizations conduct performance appraisals, few studies examine how the results are used to enhance engagement or develop employees further.

Recommendations

- **Put Continuous Feedback Systems in Place**

To keep employees motivated and informed of their accomplishments, organizations should replace annual reviews with frequent feedback sessions.

- **Make Use of AI-Powered Assessment Tools**

AI and data analytics integration can improve the

objectivity, transparency, and personalization of performance reviews.

- **Boost Communication and Leadership**

To increase engagement, leaders should keep lines of communication open, acknowledge the efforts of their staff, and promote involvement in decision-making.

- **Pay Attention to Staff Development**

To improve skills and long-term engagement, training and career development programs should be connected to performance outcomes.

- **Encourage a healthy work-life balance**

To lower stress and increase job satisfaction, which boosts engagement, companies should implement flexible work rules.

- **Encourage a Positive Workplace Culture**

Maintaining a high level of involvement and performance in the workplace is facilitated by fostering trust, inclusivity, and gratitude.

- **Regularly Assess Engagement**

Frequent surveys and engagement audits can be used to pinpoint problem areas and assess how well policies are working.

Conclusion

- Because it has a direct impact on output, job quality, and overall performance, employee engagement is a major factor in the success of a firm.
- Systems for performance evaluation assist in identifying strengths and weaknesses and give workers helpful criticism for ongoing development.
- Employee engagement lowers turnover and increases job satisfaction because engaged workers are more driven, devoted, and creative.
- Fair and transparent evaluation procedures foster confidence and guarantee that workers feel appreciated and acknowledged for their work.
- Assessments become increasingly data-driven and individualized when AI and digital tools are used to improve performance evaluation's accuracy and fairness.
- Leadership is essential; communicative and encouraging leaders keep staff members motivated and dedicated.
- Frequent praise and feedback help employees feel like they belong

and have an emotional bond with the company.

- Programs for employee training and development that are connected to performance goals support employees' personal and professional

References

- ◆ Kahn, W. A. (1990). *Psychological Conditions of Personal Engagement and Disengagement at Work. Academy of Management Journal*, 33(4), 692–724.
- ◆ Saks, A. M. (2006). *Antecedents and Consequences of Employee Engagement. Journal of Managerial Psychology*, 21(7), 600–619.
- ◆ Mone, E. M., & London, M. (2018). *Employee Engagement Through Effective Performance Management: A Practical Guide for Managers. Routledge*
- ◆ Bakker, A. B., & Demerouti, E. (2008). *Towards a Model of Work Engagement and Performance. Career Development International*, 13(3), 209–223.
- ◆ Gruman, J. A., & Saks, A. M. (2011). *Performance Management and Employee Engagement. Human Resource Management Review*, 21(2), 123–136.
- ◆ Armstrong, M. (2020). *Armstrong's Handbook of Performance Management: An Evidence-Based Guide to Delivering High Performance. Kogan Page Publishers.*
- ◆ Schaufeli, W. B., & Bakker, A. B. (2010). *Defining and Measuring Work Engagement: Bringing Clarity to the Concept. In Work Engagement: A Handbook of Essential Theory and Research. Psychology Press.*
- ◆ Gupta, V., & Kumar, S. (2015). *Impact of Performance Appraisal Justice on Employee Engagement: A Study of Indian IT Sector. Asia-Pacific Journal of Management Research and Innovation*, 11(3), 230–240.

-
- ◆ *Anitha, J. (2014). Determinants of Employee Engagement and Their Impact on Employee Performance. International Journal of Productivity and Performance Management, 63(3), 308–323.*

 - ◆ *Bailey, C., Madden, A., Alfes, K., & Fletcher, L. (2017). The Meaning, Antecedents, and Outcomes of Employee Engagement: A Narrative Synthesis. International Journal of Management Reviews, 19(1), 31–53.*

IoT- Enabled Smart Agriculture: Data Analysis and Growth Trends

SHAMAMA KAMAL¹

M.Tech Scholar
Deptt. of CSE
SRMS CET, Bareilly (U.P.)
shamamakml@gmail.com

DR. SHAILESH SAXENA²

Associate Professor
Deptt. of CSE
SRMS CET, Bareilly (U.P.)
shaileshgla@gmail.com

Abstract

The incorporation of Internet of Things (IoT) solutions in agriculture is revolutionizing traditional farming by enabling data-centric precision operations. IoT-enabled sensing, connectivity, and decision-support platforms provide real-time insights into soil, crop, and environmental conditions. This study evaluates the impact of IoT adoption in agriculture, focusing on corn and sugarcane production. Using experimental trials and secondary datasets, the findings show yield increases of 30–65%, water savings up to 50%, and input reductions such as herbicides and fertilizers. Graphical analyses and a comparative table demonstrate the agronomic and environmental benefits of IoT adoption.

Key Words: *IoT, Smart Agriculture, Precision Irrigation, Crop Yield, Datasets.*

Introduction

Global agriculture is under unprecedented pressure to meet the growing food demands of an expanding population while minimizing environmental degradation. Conventional farming methods, often characterized by uniform fertilizer application, rigid irrigation schedules, and limited monitoring of soil and crop conditions, are increasingly insufficient to achieve these goals. Such practices can lead to overuse of fertilizers, pesticides and water, contributing to soil depletion, water scarcity, and greenhouse gas emissions. In this context, the integration of advanced technologies into agriculture has emerged as a key strategy to enhancing the productivity, efficiency of resources, and sustainability. Among these technologies, the Internet of Things offers major promise by enabling precise, real-time monitoring and management of farm operations [1], [2].

IoT-enabled smart agriculture utilizes interconnected sensors, actuators, and communication technologies to gather data on soil moisture, temperature, humidity, nutrient content, and crop conditions. Then, this data is processed through cloud computing and advanced analytics to inform targeted interventions such as precision irrigation, site-specific fertilization, and early pest or disease detection. By enabling real-time, data-driven decision making, IoT systems reduce wastage, lower operational costs, and

optimize crop growth conditions. Moreover, the use of automated monitoring systems minimizes human labor requirements and enhances the predictability and efficiency of farm management practices. Such technological interventions are particularly valuable in regions with water scarcity, variable climatic conditions, or intensive crop production systems.

Corn and sugarcane, as staple and industrial crops, play a pivotal role in global food security, biofuel production, and the sugar industry. Their high economic and nutritional significance makes them ideal candidates for precision farming interventions. Studies have demonstrated that IoT-enabled solutions in corn and sugarcane cultivation can significantly increase yields, improve input-use efficiency, and reduce environmental footprints by minimizing excess water and fertilizer application [3]–[5]. As smart agriculture continues to evolve, IoT technologies are positioned to revolutionize conventional farming by creating sustainable, resilient, and highly productive agricultural systems capable of meeting the demands of the twenty-first century.

System Architecture of IoT Based Agriculture

The increasing use of IoT in agriculture is driven by improvements in internet connectivity, digital tools, and sensor technologies, has led to a continuous emergence and

corn yield compared to conventional methods. The difference between the two bars highlights the potential productivity improvement with IoT-enabled farming.

B. Sugarcane Yield under Different Irrigation Systems

Sugarcane productivity responded strongly to IoT-enabled irrigation scheduling. Trials comparing rainfed, partial irrigation (50% of available water), and full-field capacity irrigation showed that IoT-guided systems increased yields from 55 t/ha (rainfed) to 90 t/ha under optimal automated irrigation—a 63% improvement. Additionally, robotic spraying reduced herbicide usage by 35–65% while enhancing water use efficiency.

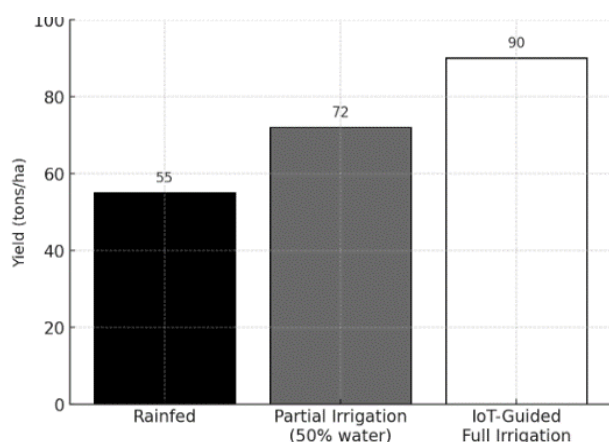


Figure 3: Impact of IoT on Sugarcane Yield

C. Comparative Table of IoT Impacts

Table 1 summarizes yield improvements, water savings, and other agronomic benefits resulting from IoT adoption.

Table 1: IoT Impacts on Corn and Sugarcane Yields and Resource Use

Crop	Corn	Sugarcane
Baseline Yield (Traditional)	7.5 t/ha	55 t/ha
IoT/Improved Practice Yield	10.0 t/ha	90.0 t/ha
Yield Increase (%)	33.3 %	63.6 %
Water Savings (%)	~30 %	~50 %
Other Benefits	Improved nutrient efficiency, early pest/disease detection [1], [2]	Reduced herbicide use (35–65%), higher WUE [3]–[5]

Discussion

The results clearly demonstrate the transformative role of IoT in modern agriculture.

A. Agronomic Benefits

- **Corn:** IoT-enabled irrigation and nutrient management improved yield by over 30% while reducing water consumption by ~30%. Early detection of pests and nutrient deficiencies enabled timely interventions, enhancing overall crop health.
- **Sugarcane:** Soil-moisture-guided irrigation and robotic input application enhanced water use efficiency, reduced herbicide use, and achieved yield increases exceeding 60%.

B. Sustainability Implications

- **Environmental:** IoT adoption minimizes water runoff, decreases soil degradation, and reduces greenhouse gas emissions by optimizing input applications.
- **Economic:** Reduced input costs and higher productivity improve farm profitability, providing incentives for adoption.
- **Social:** Smallholders gain resilience to climate variability, while technology-driven precision agriculture can support regional food security goals.

C. Challenges and Limitations

Despite clear benefits, several challenges hinder widespread IoT adoption:

- **High Initial Investment:** Sensors, cloud infrastructure, and automated systems require significant capital.
- **Digital Infrastructure:** Reliable internet connectivity is essential for real-time monitoring, which is limited in rural areas.
- **Smallholder Adoption:** Limited technical knowledge and awareness may slow adoption among small-scale farmers.

Future strategies should focus on reducing system costs, providing training, and integrating predictive analytics to maximize IoT impact across diverse farming systems.

Conclusion And Future Scope

IoT-enabled smart agriculture has shown measurable benefits by enhancing yield, optimizing resource use, and reducing input dependency. For example, corn yields improved by ~33% through IoT-based irrigation and nutrient management, while sugarcane productivity rose by more than 60% with significant reductions in herbicide use. These results demonstrate IoT's capacity to promote sustainability, efficiency, and global food security.

Moving forward, the focus should be on developing scalable and affordable solutions for smallholders, supported by distributed and interoperable IoT

development of sensors that incorporate new technologies. These sensors are evolving to be embedded, intelligent, integrated, and miniaturized. Agricultural sensors are expanding in terms of functionality, encompassing soil sensors, plant sensors, meteorological sensors and water sensors. These sensors, designed to detect a wide range of variables, provide robust support for data collection in agricultural production processes.

System architecture serves as the fundamental basis for the design and implementation of IoT-based smart agriculture systems. Consequently, researchers have carried out extensive studies on IoT architectural frameworks and have proposed various models. Most existing studies classify IoT architecture into three layers: the perception layer, the transport layer, and the application layer. However, this general layered approach has two key limitations. First, it fails to adequately represent the unique characteristics and variations of IoT technologies across specific industrial applications. Second, it does not effectively capture the diverse requirements and characteristics of different user groups.

To address this limitation, we propose five layer architecture of smart agriculture system based on IoT into five layers, which are the user layer, application layer, transport layer, perception layer, and object layer. Figure 1 depicts the function, composition and logical relationship of each layer.

To study the architecture of smart agriculture system based on IoT, the following steps should be taken:

- Identify and generalize various IoT application categories and scenarios.
- Define the core principles and requirements governing IoT architecture design.
- Elaborate on the foundational IoT architecture by specifying its framework and functional organization.

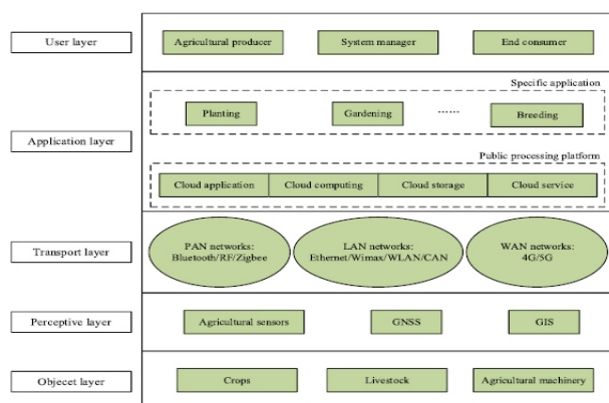


Figure 1: Architecture of Smart Agriculture Based on IoT- 6

Methodology

This study integrates secondary datasets and previously published field trials to assess the effect of IoT-enabled systems on corn and sugarcane productivity.

A. Corn (Maize)

Yield improvements under IoT-based irrigation and digital farming practices were compiled from long-term field experiments and USDA datasets [1], [2]. Parameters considered include site-specific irrigation, nutrient management, and pest/disease monitoring.

B. Sugarcane

Field experiments in Asia and Latin America were analyzed to assess irrigation scheduling, soil moisture monitoring, and robotic spraying systems [3]–[5]. IoT adoption in these trials focused on improving water use efficiency (WUE) and reducing agrochemical inputs.

C. Data Visualization

Bar graphs and comparative tables were generated to illustrate yield differences and resource savings, providing a clear visual representation of IoT impacts on crop productivity.

Results

A. Corn Yields under IoT vs Traditional Practices

Analysis of corn yields indicates significant improvements under IoT-enabled management. Figure 2 shows that traditional practices yielded 7.5 t/ha, whereas IoT-based irrigation, nutrient management, and pest monitoring increased yields to 10.0 t/ha, representing a 33% improvement.

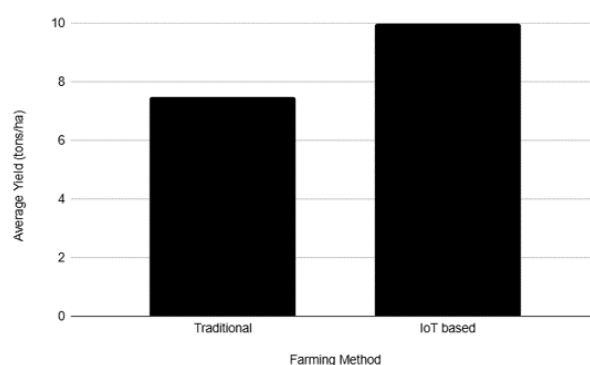


Figure 2: Comparison of Corn Yield with Traditional Farming vs IoT based Farming.

The chart visually demonstrates that integrating IoT technology into farming practices can significantly increase

architectures that enable seamless data sharing and integration across systems. Research must address perception standards, embedded gateways, and multi-protocol conversions to build robust agricultural IoT ecosystems. Furthermore, the convergence of IoT with advanced technologies such as 5G, VR, AR, and machine learning can establish digital twins of agricultural processes, enabling predictive decision-making, immersive simulations, real-time monitoring, and multi-factor traceability. Together, these advancements will transform agriculture into a highly intelligent, sustainable, and resilient sector, benefitting both farmers and consumers worldwide.

References

- ◆ M. K. R. Muditha et al., “Digital agriculture increases corn yield by 31% over 10 years,” *Agricultural Systems*, vol. 196, p. 103328, 2022.
- ◆ H. H. Al-Ghobari and M. M. Dewidar, “Smart irrigation systems for maize: yield and water productivity improvements,” *Irrigation Science*, vol. 39, pp. 45–56, 2021.
- ◆ R. S. Inman-Bamber et al., “Strategies for improved sugarcane water use efficiency,” *Field Crops Research*, vol. 246, p. 107701, 2020.
- ◆ J. M. Torres-Sánchez et al., “Soil-moisture guided irrigation improves sugarcane yield and WUE in Nicaragua,” *Agricultural Water Management*, vol. 228, p. 105882, 2020.
- ◆ A. P. R. Rodrigues et al., “Selective robotic spraying in sugarcane: Reducing herbicide input by 35–65%,” *Precision Agriculture*, vol. 25, no. 1, pp. 87–102, 2024.
- ◆ Xu, J., Gu, B., & Tian, G, 2022, “Review of agricultural IoT technology”, *Artificial Intelligence in Agriculture* 6 (2022)

Submission of Manuscript

Bizcraft is a halfyearly journal on contemporary management perspectives published by the Faculty of management Science, SRMS College of Engg & Tech, Bareilly (UP), India . It invites original research articles, case study, executive deliberation, book reviews and perspective based papers from academicians and practitioners on any issue of management and technology perspectives. The author should send two print copies of manuscript on A4 size paper with double line space on Times New Roman 12 point fonts on MS Word format. Sufficient left margin must be available on all the pages for facilitating the review of the article by the reviewer. The review process normally takes one month from the date of receiving of the article by the editor. The unaccepted articles will not be returned.

One soft copy must also be mailed to bizcraft@srmscet.edu.

The manuscripts should be arranged in following order :

1. Cover page consisting the title of the submitted articles along with the name (s) of the contributor(s), his/her designations and brief profile of each contributor(s) along with contact address. It must consists a declaration that “It is certified that the manuscript titled “Title” which is submitted for publication in Bizcraft. A half yearly journal of Faculty of Management Sciences, Shri Ram Murti Smarak College of Engg & Tech, Bareilly (UP), India is my original work and all references and source of data and conclusions are properly acknowledged”.
2. Abstract in around 100-150 words briefly explaining the theme of the contributed manuscript, its relevancy in contemporary management practices and research methodology, which is used for preparation of the article (if applicable).
3. The article itself in around 6000 to 10000 words depending upon the aspect of issue presented in the manuscript. It may include the innovative thought with its practical applicability, conducted research work, case study, book review etc. The data table, graphs and charts etc. must be numbered properly and attached as separate sheet with clear presentation

The acceptance of the article for publication is based on the understanding that the manuscript is an unpublished work and not submitted for publication anywhere else. The editorial board reserved the right for suitable modification in the article.

Guidelines for references :

It is suggested that all type of data and conclusions must be properly acknowledged in term of its source in proper format. The references must be arranged in alphabetical order mentioning the name of the researcher/source. For example Hedge, L.V (1995). “Statistical Method for Meta Analysis”, Journal of Statistical Research, Vol no, Page No. for referring the journals or published works. Standard format may also be used for referring the books and working papers.

Editor reserves the right to accept or refuse an article for publication, and there is no obligation to assign reasons for the decision. The author will receive a complementary copy of the Bizcraft in which their article is published.

All Manuscript should be submitted to :

The Editor

Bizcraft

Faculty of Management Science

SRMS College of Engg. & Tech.

Ram Murti Puram, 13 KM. Bareilly-Nainital Road, Bareilly-243202, Uttar Pradesh, India

Ph : 0581-2582246, 2582249, E-Mail : bizcraft@srmscet.edu



ISSN : 2231- 0231



Published by :

Faculty of Management Science
Shri Ram Murti Smarak College of Engg. & Tech., Bareilly (U.P.) India