IITM Journal of Information Technology

Volume 11 (January - December 2025)
ISSN No. 2395 – 5457
Special Issue

IITM
Nurturing Excellence

INSTITUTE OF INNOVATION IN TECHNOLOGY & MANAGEMENT
Affiliated to GGSIPU, NAAC Grade 'A', ISO 14001:2015, 17020:2012,
21001:2018 & 50001:2018 Certified, A Grade by GNCTD, A Grade by SFRC

IITM Journal of Information Technology

IITM Journal of Information Technology is a National Annual Journal of Information Technology intended for professionals and researchers in all fields of Information Technology. Its objective is to disseminate experiences, ideas, case studies of professionals in Information Technology to propagate better understandings. Its focus is on empirical and applied research and reflections that are relevant to professionals of Information Technology with academic standards and rigor within the purview. The views expressed in the Journal are those of the authors. No part of this publication may be reproduced in any form without the written consent of the publisher.The Journal intends to bring together leading researchers and Information Technology practitioners from around the country.

IITM Journal of Information Technology

Annual Journal of Institute of Innovation in Technology & Management

Volume 11 **January - December, 2025**

CONTENTS

Research Papers & Articles

Intelligent Computing for Wireless Sensor Networks : A Survey

Meenu[1], Deepti Sharan[2],Priya Tripathi[3]
[1,3]Computer Science Department, IINTM ,Janakpuri New Delhi, [2]Computer Science Department,
AUM Education Society,USA
[1]drmeenu.knsl@gmail.com, [2]deepti.sharan@gmail.com, [3] priyatripathi.iitm@gmail.com

Abstract: Wireless sensor networks (WSNs) consist of distributed, autonomous devices that collaboratively monitor and sense physical or environmental conditions. WSNs encounter several challenges, primarily due to communication failures, computational and storage limitations, and constrained power resources. In recent years, computational intelligence (CI) paradigms have been successfully employed to address various issues such as data aggregation and fusion, energy-efficient routing, task scheduling, security, optimal deployment, and localization. CI offers adaptive mechanisms that demonstrate intelligent behavior in complex and dynamic WSN environments, providing flexibility, autonomy, and robustness against topology changes, communication disruptions, and evolving scenarios.

However, WSN developers often lack awareness or a comprehensive understanding of the potential of CI algorithms. Conversely, CI researchers may not be fully familiar with the practical challenges and specific requirements of WSNs. This disconnects hampers collaboration and innovation. To bridge this gap, this paper provides an in-depth introduction to WSNs and their characteristics. It also presents an extensive review of CI applications across various WSN-related challenges, drawing insights from diverse research fields and publication sources. Additionally, the paper discusses the advantages and limitations of CI algorithms compared to traditional WSN approaches and offers a general evaluation of CI algorithms as a guide for their application in WSNs.

Keywords: Wireless Sensor Network, Computational Intelligence, Clustering Algorithms

1. Introduction

A wireless sensor network (WSN) comprises distributed, autonomous devices that cooperatively sense or monitor physical and environmental conditions [1]. WSNs are utilized in diverse applications, including environmental monitoring, habitat tracking, natural disaster prediction and detection, medical monitoring, and structural health assessment [2]. These networks consist of numerous small, low-cost, disposable, and self-sufficient sensor nodes, typically deployed ad hoc across large geographical areas for remote operations.

Sensor nodes face significant constraints, such as limited storage, computational power, communication bandwidth, and energy supply. Generally, sensor nodes are organized into clusters, with each cluster having a designated cluster head. The cluster head aggregates data from the nodes and forwards it to a specialized node, known as a sink node or base station, via multi-hop wireless communication, as illustrated in Figure 1. However, some WSNs may be simpler, consisting of a single cluster with one base station [3]–[5]. Other configurations, such as networks with multiple base stations or mobile nodes, are also possible. Article [6] provides a classification of WSNs based on communication functions, data delivery models, and network dynamics.

Resource limitations and dynamic topologies introduce challenges in areas such as network discovery, control and routing, collaborative data processing, querying, and task assignment [2]. Computational intelligence (CI) incorporates principles of learning, adaptation, evolution, and fuzzy logic to create intelligent systems. Beyond paradigms like neural networks, reinforcement learning, evolutionary algorithms, and fuzzy systems, CI also includes approaches such as swarm intelligence, artificial immune systems, and hybrid methodologies.

CI paradigms have found practical applications in fields like product design, robotics, intelligent control, biometrics, and WSNs. Researchers have successfully applied CI techniques to address numerous challenges in WSNs. However, these applications are being developed across various research communities, with no unified overview of the work. Most of the contributions are scattered across journals and conferences that do not primarily focus on WSNs.

The objective of this survey is to bridge this gap by providing a concise yet comprehensive overview of various CI approaches and their applications, offering WSN researchers fresh perspectives and inspiration. Additionally, the survey highlights unresolved challenges in WSNs and explores potential CI applications, aiming to motivate researchers to integrate CI techniques into WSN-related studies and developments.

2. Literature Review

This survey aims to provide a comprehensive overview of the application of computational intelligence (CI) techniques to address challenges inherent in wireless sensor and actuator networks (WSANs). Despite both CI and WSANs being active research domains, they are seldom explored together in a unified context. To the best of our knowledge, this is the first systematic review that categorizes, analyzes, and compiles CI applications within the WSAN field, effectively bridging the gap between these two complementary paradigms.

While some existing works delve deeply into specific niche areas relevant to our survey, research explicitly linking CI to WSANs remains limited. Survey papers and books focusing on WSANs [11–15] are relatively scarce compared to those addressing WSNs as a whole [16–18] or targeting specific WSN problems [19–24]. Even in studies where CI methods are used, they are often not the primary focus.

Some researchers have highlighted the use of specific CI methods in addressing particular WSN challenges [25, 26], while others have examined how a single CI technique applies to multiple WSN-related problems [27–34]. Although valuable, these studies are narrower in scope and do not emphasize WSANs. This survey builds upon these contributions to present a broader and more holistic perspective, specifically tailored to the WSAN domain.

3. Challenges In Sensor Networks

Real-world deployments of wireless sensor networks (WSNs) typically support one of three primary applications: periodic reporting, event detection, and database-like storage. **Periodic reporting**, the simplest and most common scenario, involves sensors sampling the environment at regular intervals, storing the data, and transmitting it to base stations. These networks often connect to actuators, such as automatic irrigation or alarm systems, and are widely used in monitoring applications like agriculture [7,8], microclimate [4,5,9], habitat surveillance [10–12], military operations [13], and disaster relief [14]. A key characteristic of periodic reporting is its predictable data traffic and volume.

In contrast, **event detection** applications [3,15] operate by sensing the environment and immediately evaluating the data for significance. If an event is detected, the data is sent to the base station, resulting in sporadic and unpredictable data traffic. Even when no events occur, nodes exchange minimal data for route management and status checks.

Database-like storage systems [16], similar to event-based systems, store all sensory data—whether periodic samples or event-triggered readings—locally on nodes. Base stations then query and retrieve the required data directly from the nodes. The main challenge here is implementing efficient data storage and retrieval mechanisms.

Challenges in WSN Deployments

WSNs face several deployment-specific challenges:

3.1 Wireless Ad Hoc Nature

➢ **Characteristics:** WSNs lack fixed communication infrastructure and rely on shared wireless media, which introduces issues like unreliable and asymmetric links. However, the broadcast advantage allows packets sent to one node to be received by all its neighbors.

3.2 Mobility and Topology Changes

➢ **Characteristics:** Nodes may join, leave, move, or fail, causing dynamic topology changes. Networks must remain robust to such disruptions.

3.3 Energy Constraints

➢ **Characteristics:** Nodes operate on limited energy, often with no possibility of battery replacement or recharging. Communication tasks consume the most power, necessitating energy-efficient protocols.

3.4 Physical Distribution

- **Characteristics:** Data is distributed across nodes, making global information gathering costly. Decentralized algorithms are essential to reduce communication overhead.

Key Challenges Addressed by CI Techniques

- **Design and Deployment**

WSNs serve varied applications, from tissue-implanted sensors to forest-fire monitoring. Deployment strategies vary, requiring tailored designs to optimize node type, quantity, and placement.

- **Localization**

Localization ensures nodes are aware of their positions, critical for event detection and geometric-aware routing [17,18]. Common methods involve time-of-arrival signals from multiple base stations [19,20].

- **Data Aggregation and Sensor Fusion**

Sensor fusion combines data from multiple nodes to enhance accuracy or reduce communication overhead. Techniques like Kalman filters and Bayesian networks are commonly used [21,22].

- **Energy-Aware Routing and Clustering**

Efficient energy use is crucial for extending network lifetime. Hybrid routing protocols and hierarchical clustering are effective strategies for managing densely deployed networks [23].

- **Scheduling**

Energy conservation requires nodes to operate on strict schedules, alternating between sleep and active modes. Scheduling ensures efficient sensing, transmission, and locomotion while maximizing network lifespan.

- **Security**

Wireless links are vulnerable to threats like eavesdropping, impersonation, and message tampering. Robust security measures, including encryption and intrusion detection, are critical for maintaining network integrity [24].

- **Quality of Service (QoS) Management**

QoS refers to ensuring application-specific service attributes like fairness, delay, bandwidth, and packet loss. Networks must balance QoS with resource optimization to meet user expectations [27].

These challenges and their solutions underscore the importance of integrating advanced techniques, including computational intelligence, to enhance WSN performance and reliability across diverse applications.

4. Computational Intelligence Techniques

Computational Intelligence (CI) is a smart computational approach that employs heuristic algorithms to efficiently derive approximate solutions for NP-hard problems. CI paradigms are well-suited for adapting to the dynamic and evolving nature of WSNs. The following subsections provide a brief overview of several CI paradigms applied to clustering in WSNs.

4.1 Genetic Algorithm

Inspired by Charles Darwin's theory of evolution, specifically the concept of "survival of the fittest," Genetic Algorithm (GA) was formally introduced by John Holland in the 1970s [30]. GA is an adaptive heuristic search algorithm that simulates the process of biological evolution. Renowned for its robustness, it operates by exploring a population of potential solutions and has demonstrated remarkable flexibility in addressing dynamic and NP-hard problems.

The primary challenge in applying GA lies in encoding the problem into a set of chromosomes, where each chromosome represents a potential solution. The quality of these chromosomes is assessed using a fitness function. Based on their fitness values, selected chromosomes undergo crossover and mutation processes.

The **crossover** process generates new solutions, or offspring, by combining segments of two parent chromosomes. The **mutation** process introduces changes to one or more genetic elements in the offspring to maintain diversity and avoid convergence to local minima. This combination of techniques allows GA to explore the solution space effectively and adapt to complex problem scenarios.

Algorithm 1 : Basic steps describing the GA [31]

```
begin GA
for all N chromosomes
Initialize the population,generation counter
```

```
    Initialize the GA parameters.
    Calculate the fitness of each chromosome.
end for
while (the convergence condition is not satisfied) or
(the maximum number of iterations is not reached)
{
    for all created N offsprings
        Probabilistically select a pair of chromosomes
        from current population using the fitness value.
        Produce a new offspring xi using crossover
        and mutation operators,where i = 1, 2, . . . ,N.
        Evaluate the population.
    end for
    Replace current population with newly created one.
    Update the generation counter.
}
end while
end GA
```

4.2 Particle Swarm Optimization

Particle Swarm Optimization (PSO) was developed in 1995 by James Kennedy and Russell Eberhart [32]. PSO is a powerful stochastic nonlinear optimization technique inspired by the movement and intelligence of swarms. It draws from the social behavior of birds or fish, where a group of birds searches for food in an area by following the bird nearest to it. PSO combines local and global search strategies through social interactions among particles, helping them find the best positions achieved so far.

PSO and Genetic Algorithm (GA) share similarities [33], as both are population-based stochastic optimization methods that begin with a randomly generated population. Both methods use fitness values to evaluate and update the population in search of an optimal solution through random techniques. However, PSO differs from GA in several ways: it lacks crossover and mutation processes, and particles do not "die." Instead, they update their positions based on internal velocities. Additionally, the information-sharing mechanism in PSO is quite distinct.

In PSO, each particle represents a point in a multi-dimensional space and updates its position influenced by two components: the cognitive component, which reflects the particle's individual experience, and the social component, which is derived from communication with neighboring particles. The fundamental PSO equations are presented in Equations 1 and 2, with several enhancements to the standard PSO model outlined in [34].

Algorithm 2: Basic steps of the PSO algorithm

```
begin PSO
    Randomly initialize the position and velocity of
    the particles: Xi(0) and Vi(0)
    while (While terminating condition is not reached) do
        for for i = 1 to number of particles
            Evaluate the fitness:= f(Xi)
            Update pi and gi
            Update velocity of the particle Vi
            Update position of the particle Xi
            Evaluate the population fitness
        Next for
    end while
end PSO
```

The steps of the PSO process are outlined in Algorithm 2. The selection of the communication neighborhood, known as the swarm topology, plays a crucial role in the model's implementation. In a Star topology, all particles in the swarm communicate with each other, while in a Ring topology, each particle interacts only with two neighboring particles. While the Star topology can lead to faster convergence, this can sometimes be misleading, as it may result in premature convergence. On the other hand, the Ring topology tends to exhibit slower convergence and is less prone to premature convergence, making it more effective for multimodal problems. Various topologies have been proposed and discussed in [35].

Table 1: Overview different type CI Technique

Type of CI Techniques	Computational Complexity	Application Scenario	Example
Fuzzy Logic	Low	Reasoning with vague and imprecise concepts	Fuzzy controller for a plant irrigation system [31]
Learning Systems	Medium	Learning relationships among objects	Learning foraging behaviors in a robotic swarm [32]
Evolutionary Algorithm	Medium	Finding approximate solutions to challenging optimization problems	Calculating near-optimal path for data collection by a mobile sink [33]
Swarm Intelligence Algorithm		Finding approximate solutions to challenging optimization problems	Minimizing localization error of the sensors via a mobile anchor node [34]
Hybrid Systems	High	Combining the strengths of complementary techniques	Improve QoS metrics in a WSAN [35]

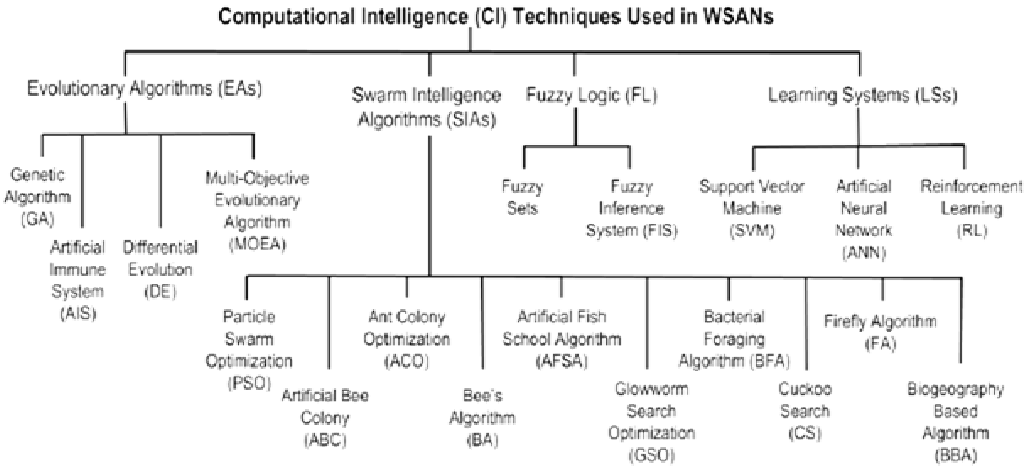

Computational Intelligence (CI) Techniques Used in WSANs
Evolutionary Algorithms (EAs)
Swarm Intelligence Algorithms (SIAs)
Fuzzy Logic (FL)
Learning Systems (LSs)
Genetic Algorithm (GA)
Artificial Immune System (AIS)
Differential Evolution (DE)
Multi-Objective Evolutionary Algorithm (MOEA)
Fuzzy Sets
Fuzzy Inference System (FIS)
Support Vector Machine (SVM)
Artificial Neural Network (ANN)
Reinforcement Learning (RL)
Particle Swarm Optimization (PSO)
Artificial Bee Colony (ABC)
Ant Colony Optimization (ACO)
Bee's Algorithm (BA)
Artificial Fish School Algorithm (AFSA)
Glowworm Search Optimization (GSO)
Bacterial Foraging Algorithm (BFA)
Cuckoo Search (CS)
Firefly Algorithm (FA)
Biogeography Based Algorithm (BBA)

Fig 1: CI techniques used in the surveyed WSAN papers

5. Methodology (Ci Techniques Applied to Wsan Problems)

Wireless Sensor and Actuator Networks (WSAN) are collections of static sensor nodes and one or more sink nodes. The often-numerous sensor nodes are composed of one or more sensing modules, an energy source and a wireless communication device. The sensor nodes in these networks usually have limited computational power, thus requiring multihop chains to transmit their messages across the network to the sink nodes. WSNs are prone to node failure due to malfunction, energy depletion, malicious attacks or harsh environmental conditions. An extension of such networks is called Wireless Sensor and Actuator Networks (WSANs), which are made up of heterogeneous nodes capable of performing distributed computations and actuation tasks [25].

The WSAN Actuation problem category has been tackled from many standpoints using CI techniques. Those approaches that revolve around Task Allocation often resort to market-based allocation techniques optimized via EAs/SIAs to satisfy the overall system goal. There is plenty of room for the application of MOO methods in this area. Another popular trend is to employ FIS/ANN to design control systems for these actuators that allow them to individually bid for certain tasks. Regarding the subset of Actuation approaches concerned with task execution via actuator coordination and event prediction, FIS and FL are the main CI schemes employed to ensure a smooth coordination among the actuators, although we see an emerging interest in RL and MDP as LS representatives.

The optimization angle is still present via EAs/SIAs solving different manifestations of actuator coordination problems such as target tracking or path planning. A vast majority of the proposed approaches rely on a centralized computation architecture.

In the WSAN Communication category, the application of CI techniques to the routing subproblem is confined to solving optimization problems primarily via SIAs. The communication routes are mainly static (i.e., do not change over time) except that envisions dynamic communication backbones. Multiple aspects of these routes such as energy consumption, signal strength or message latency are taken into account during the optimization process. In the clustering subproblem, the suitability of a WSAN node to become a cluster head is modeled through an FIS and the selection of potential cluster heads network-wise is entrusted to EA-based optimizers. Finally, the QoS sub-problem is the least explored by CI techniques. The few available works are related to fuzzy control and genetic optimization at the node level to ensure reliable sensor-actuator communication.

Concerning the Sink Mobility category, CI optimization techniques have the upper hand as they try to derive the best path for the mobile sink. Some studies simultaneously identify the most suitable cluster heads in the WSAN. A few works depart from the traditional problem formulation by considering special cases such as multiple mobile sinks or a sparse network. Finally, an FIS to gauge the attractiveness of the network regions for sink visitation was also put forth. MOO methods as well as LS/HS schemes would be a great addition to the repertoire of CI applications here.

The CI presence in the WSAN Topology Control category is largely dominated by EA/SIA-based optimization methods across all its subproblems, namely sensor deployment, relocation and replenishment. This is quite understandable since modifying the WSAN topology serves an ultimate goal, e.g., maximizing network lifetime or expanding/restoring network coverage. We do see increasing evidence of the successful synergy between FIS/DL and nature-inspired CI optimizers in the sensor relocation arena. Sensor replenishment by mobile actuators is an exciting and largely uncharted territory for new CI applications.

Finally, in the WSAN Localization problem, we notice that range-based methods have been slightly more studied through CI techniques than their range-free counterparts. The need to reason under imprecise information (coming from unreliable distance estimates of the nodes) makes it an appealing choice for the application of FL/FIS and LS (ANN/SVM) techniques,

with some genetic and swarm-inspired optimizers in the background to produce an accurate solution. The latter category (range-free localization methods) hinges more heavily on EA/SIA-based optimization given the rather reliable estimates of the anchor nodes' position that are broadcast to the rest of the WSAN.

6. Conclusions And Future Applications Of Ci In Wsns

Recent literature shows that researchers have focused their attention on innovative use of CI techniques to address WSN issues such as design and deployment, localization, security, optimal routing and clustering, scheduling, data aggregation and fusion, and QoS management. Recent implementations of CI methods in various dynamical and heterogeneous networks are presented in this survey paper. CI paradigms and numerous challenges in sensor networks are briefly introduced, and the CI approaches used by researchers to address the challenges are briefly explained. In addition, a general evaluation of CI algorithms is presented, which will serve as a guide for using CI algorithms for WSNs.

An advanced CI approach called adaptive critic design holds promise to generate practical optimal/sub-optimal solutions to the distributed sensor scheduling problem. There are successful applications of adaptive critic designs in power systems, which show that the technique provides guaranteed stable optimal solutions under uncertainties and noise. The potential of adaptive critic designs remains to be exploited in the field of WSN scheduling

References

1. I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.
2. C. Y. Chong and S. Kumar, “Sensor networks: Evolution, opportunities,and challenges,” *Proc. IEEE*, vol. 91, no. 8, pp. 1247–1256, Aug. 2003.
3. G. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees,and M. Welsh, “Deploying a wireless sensor network on an active volcano,” *IEEE Internet Comput.*, vol. 10, no. 2, pp. 18–25, 2006.
4. K. Martinez, P. Padhy, A. Riddoch, R. Ong, and J. Hart, “GlacialEnvironment Monitoring using Sensor Networks,” in *Proc. 1st Workshop Real-World Wireless Sensor Netw. (REALWSN)*, Stockholm, Sweden, 2005, p. 5.
5. I. Talzi, A. Hasler, S. Gruber, and C. Tschudin, “Permasense:Investigating permafrost with a WSN in the swiss alps,” in *Proc. 4th Workshop Embedded Netw. Sensors (EmNets)*, Cork, Ireland, 2007, pp.8–12.
6. S. Tilak, N. B. Abu-Ghazaleh, and W. Heinzelman, “A taxonomy of wireless micro-sensor network models,” *SIGMOBILE Mob. Comput.Commun. Rev.*, vol. 6, no. 2, pp. 28–36, 2002.
7. A. Nayak and I. Stojmenovic, Wireless sensor and actuator networks:algorithms and protocols for scalable coordination and data communication.Wiley, 2010.
8. R. Verdone, D. Dardari, G. Mazzini, and A. Conti, Wireless sensorand actuator networks: technologies, analysis and design. AcademicPress, 2010.
9. R. Falcon, “Towards fault reactiveness in wireless sensor networks with mobile carrier robots,” Ph.D. dissertation, University of Ottawa, 2012.
10. N. Mitton and D. Simplot-Ryl, Wireless sensor and robot networks:from topology control to communication aspects. World Scientific,2013.
11. D.-I. Curiac, “Towards wireless sensor, actuator and robot networks:conceptual framework, challenges and perspectives,” ournal of Networkand Computer Applications, vol. 63, pp. 14–23, 2016.
12. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer networks, vol. 38, no. 4, pp.393–422, 2002.
13. P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, and Y. F. Hu,“Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and zigbee standards,” Computer communications, vol. 30,no. 7, pp. 1655–1695, 2007.
14. Y.-G. Yue and P. He, “A comprehensive survey on the reliability of mobile wireless sensor networks: Taxonomy, challenges, and futuredirections,” Information Fusion, 2018.
15. J. N. Al-Karaki and A. E. Kamal, “Routing techniques in wireless sensor networks: a survey,” IEEE wireless communications, vol. 11,no. 6, pp. 6–28, 2004.

16. J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” Computer Networks, vol. 52, no. 12, pp. 2292–2330, 2008.

17. M. Younis and K. Akkaya, “Strategies and techniques for node placement in wireless sensor networks: A survey,” Ad Hoc Networks, vol. 6 no. 4, pp. 621–655, 2008.

18. G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, “Energy conservation in wireless sensor networks: A survey,” Ad hoc networks,vol. 7, no. 3, pp. 537–568, 2009.

19. M. Xie, S. Han, B. Tian, and S. Parvin, “Anomaly detection in wireless sensor networks: A survey,” Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1302–1325, 2011.

20. I. Khoufi, P. Minet, A. Laouiti, and S. Mahfoudh, “Survey of deployment algorithms in wireless sensor networks: coverage and connectivity issues and challenges,” International Journal of Autonomous and Adaptive Communications Systems, vol. 10, no. 4, pp. 341–390, 2017.

21. K. Langendoen, A. Baggio, and O. Visser, “Murphy loves potatoes:experiences from a pilot sensor network deployment in precision agriculture,” in Proc. 20th Int. Symp Parallel Distributed Proc. Symp.(IPDPS), Rhodes Island, Greece, 2006.

22. J. McCulloch, P. McCarthy, S. M. Guru, W. Peng, D. Hugo, and A. Terhorst, “Wireless sensor network deployment for water use efficiency in irrigation,” in Proc. Conf. Workshop Real-world Wireless Sensor Netw. (REALWSN), Glasgow, Scotland, 2008, pp. 46–50.

23. E. A. Basha, S. Ravela, and D. Rus, “Model-based monitoring for early warning flood detection,” in Proc. Conf. 6th ACM Conf. Embedded Netw. Sensor Syst. (SenSys), New York, NY, USA, 2008, pp. 295–308.

24. G. Barrenetxea, F. Ingelrest, G. Schaefer, and M. Vetterli, “The hitchhiker's guide to successful wireless sensor network deployments,” in Proc. 6th ACM Conf. Embedded Netw. Sensor Syst. (SenSys), New York, NY, USA, 2008, pp. 43–56.

25. T. Naumowicz, R. Freeman, A. Heil, M. Calsyn, E. Hellmich, A. Braendle, T. Guilford, and J. Schiller, “Autonomous monitoring of vulnerable habitats using a wireless sensor network,” in Proc. 3rdWorkshop Real-World Wireless Sensor Netw. (REALWSN), Glasgow, Scottland, 2008, pp. 51–55.

26. R. Szewczyk, J. Polastre, A. Mainwaring, and D. Culler, “Lessonsfrom a sensor network expedition,” in Proc. 1st European Workshop Sensor Netw. (EWSN), Berlin, Germany, 2004, pp. 307–322.

27. X. Peng, Z. Mo, L. Xiao, and G. Liu, “A water-saving irrigation system based on fuzzy control technology and wireless sensor network,” Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1–4, 2009.

28. J. Timmis, L. Murray, and M. Neal, “A neural-endocrine architecture for foraging in swarm robotic systems,” Studies in omputationalIntelligence, vol. 284, pp. 319–330, 2010.

29. J. S. Liu, S. Y. Wu, and K. M. Chiu, “Path planning of a data mule in wireless sensor network using an improved implementationof clustering-based genetic algorithm,” Proceedings of the IEEE Symposium on Computational Intelligence in Control and Automation, pp. 30–37, apr 2013.

30. S. Sivakumar and R. Venkatesan, “Error minimization in localizationof wireless sensor networks using modified cuckoo search with mobile anchor positioning (MCS-map) algorithm,” International Journal of Computer Applications, vol. 95, no. 6, 2014

31. M. Hamdy and H. El-Madbouly, “Improvement of QoS management in wireless sensor/actuator networks using fuzzy-genetic approach,”Proceedings of the International Conference on Networking and MediaConvergence, pp. 29–35, mar 2009.

Expansion of AI in Stock Trading: A Growing Trend

Narinder K. Seera[1,] Jaspreet Kaur[2]

[1]Department. of Computer Science, IINTM, N. Delhi, [2]University of Westminster, London, U.K

[1]narinderkaur.ipu@gmail.com,[2] jaspreet.westminster@gmail.com

Abstract - The massive rise of AI in different domains, including financial institutions such as banks, stock exchange market, is empowering stakeholders to make informed decisions based on AI-driven tools & technologies. Employing AI in stock trading is not a new term, but it has certainly covered a long journey. These days Artificial intelligence trading strategies are playing a crucial role in market analysis, price prediction, stock selection, investment planning, portfolio management, etc. This paper is an attempt to explore the role of AI in stock trading with various types of trading options and portfolio management using AI based tool. It also throws light on recent developments in this field.

Keywords -Stock trading, Artificial Intelligence (AI), portfolio management, AI trading strategies

1. Introduction

Through the inception of Artificial Intelligence and its subsequent technological innovations over the last decade has significantly transfigured the way different functions and operations are performed in different sectors. With the expansion of AI technologies from IT industry to IoT, from organizations to educational institutes, from medical or health sector to banking sector, all have realized a drastic change in various operations that are being performed. Stock trading in financial market is also one of the areas which is greatly impacted by the potential of AI technologies which has changed the way securities are actively traded and stocks are sold or bought.

The financial markets are taking significant advantages with the use of AI. In stock trading, AI is being used to make effective financial decisions [7]. AI techniques are employed to identify and capture underlying relationships between large data sets to make decisions regarding intelligent asset allocation and stock selection. In this paper, we explore how AI has transformed different investment strategies and types of trading. We also delve into the benefits and risks associated with the use of AI in trading.

Technically speaking, AI trading utilizes deep learning algorithms and AI techniques to analyze market data and patterns [8]. It uses novel techniques from deep learning, machine learning, natural language processing, computer vision, etc. to analyze stock data to identify patterns and predict market trends. The model is trained using machine learning (ML) techniques to predict future price movements and trade in the market. AI technology processes and analyses large volumes of data to identify patterns, exploit market inefficiencies, and optimize trading strategies for increased accuracy and efficiency [9]. It improves the efficiency of decision-making by reducing human intervention and shortsightedness. With this improvement, buying and selling stocks is stress-less and efficient. Recent studies show that around 80% of the total trading volume is initiated through algorithmic trading.

Integrating AI into investment portfolios is no longer reserved for tech giants and hedge funds. However, from stock selection algorithms to machine learning models that predict market trends, AI tools have become far more available to retail investors. These technologies can process vast amounts of data, help allocate portfolios, manage risk, and even provide personalized investment advice. In the subsequent sub-sections we discuss the functions of AI and types of trading.

1.1 Key functions of AI in stock trading

The technological advancement of AI in trading provides individual investors and traders with deep insights and analytics which were earlier available to large firms only [1]. As an instance, AI systems can analyze sentiments on social media and news articles, allowing investors to gauge market sentiment and make informed decisions. This analysis allows retail investors to make better-informed choices, enhancing their investment strategies [10]. To perform this analysis, AI algorithms go through various operations which are mentioned below:

➢ **Data Gathering:** Collecting significant financial data from various internet sources like social media, sentiments, corporate financials, news stories, trends and patterns available on portals and historical pricing data.

- **Data Preprocessing:** This step is crucial for cleaning and transforming the obtained data to ensure consistency and accuracy before training AI models.
- **Feature Engineering:** This step involves identifying relevant features from the dataset with predictive value, to be used in the training.
- **Selecting an appropriate algorithm:** Among a bunch of available ML and NLP algorithms, selecting a suitable algorithm for accurate stock trading is important.
- **Training the Model:** The most important step is to train the model in order to derive patterns and connections in the market.
- **Live Trading:** It ensures implementation of AI models for real-time trading ensuring risk management procedures are in place in order to guard against unexpected market movements.
- **Continuous Optimization:** The last but not the least, a never ending task is to continuously keep adapting and learning from current data to stay updated and effective in the ever-changing market landscape.

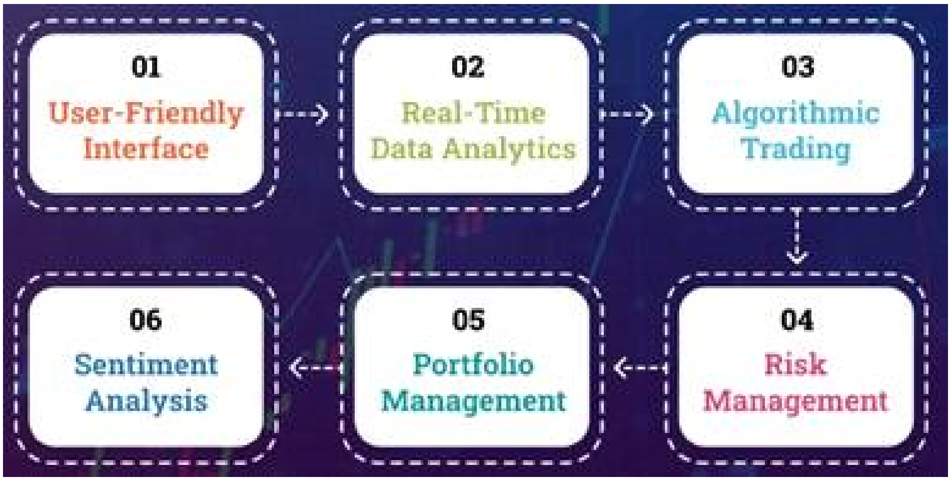


Fig. 1: Roles of AI in Stock Trading

1.2 Types of AI Trading

AI has expanded itself deep into trading and thus it can be categorized into four primary types:

- **Quantitative Trading:** This trading strategy examines price and volume data to find out the most profitable investment opportunities. This strategy is built on the fundamentals of statistics, mathematical models, data analysis, and machine learning algorithms. Its main aim is to analyze patterns, anomalies, and trends within financial markets to gain an in-depth insight of trading. The main advantages offered by this type of trading are – high speed and efficiency, elimination of emotional bias, robust risk management etc.
- **Algorithmic Trading:** It is the practice of purchasing or investing according to some prescribed set of rules tested on historical data or trends. In this type of trading, the traders make use of predetermined rules based on historical data to make trading decisions. These sets of rules are based on charts, indicators, technical analysis or stock essentials. For example, assume you have a proposition to purchase a particular stock presuming that the stock will end up in losses for next five consecutive days before its price rises. In this case, one can build an algorithm in such a way that the buy order for the particular stock is met when price touches a pre specified low point and sold when the price meet at its pre specified high point.
- **High-frequency Trading:** It falls under a subset of algorithmic trading strategy which involves frequently buying and selling large volumes of stocks. It is called high-frequency trading (HFT) as huge volumes of stocks and shares are sold and bought mechanically at very high speeds. Recently, it has been noticed that many regular stock market investors have moved towards HFT. It is predicted that it will become the most authoritative form of algorithmic trading in the future.

- **Automated Trading: It** automatically creates and submits order to stock market, eliminating the need of human intervention. The whole process begins with the defining the predefined rules for trade entries and their respective exit criteria [6]. On the basis of these predefined rules, strategies are formulated in online automated trading system. Once the system is finally set up, it continuously monitors the fluctuations in the real markets and hence searching for prospects where there could be a match for the predefined criteria. When the desired conditions are met, the trading system automatically runs the trade, including placing market orders, limit orders, or even more complex multi-leg options strategies. The entire process is shown in Figure 2.

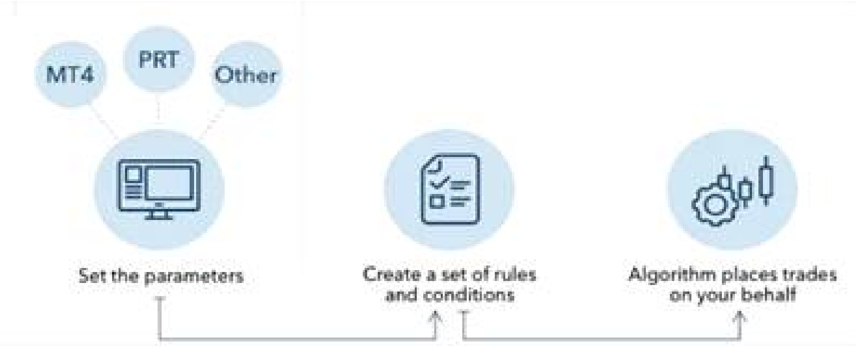

MT4
PRT
Other
Set the parameters
Create a set of rules and conditions
Algorithm places trades on your behalf

Fig. 2: How Automated Trading Works [11]

2. Using AI in Portfolio Management

With AI technologies, portfolio management and decision making in algo trading for asset allocation can be enhanced. AI can efficiently analyze market trends, economic indicators, and corporate data to suggest suitable portfolio adjustments that are helpful in risk management and mitigation [3]. These AI based technologies include machine learning models that can understand huge volumes of data more swiftly and accurately than any human can do. AI frameworks for stock trading can also oversee diverse portfolios across various asset categories, thereby ensuring that the distribution matches the investor's risk preferences and strategic goals. This automated, data-driven approach helps maintain a balanced portfolio that can adapt to market changes and capitalize on emerging opportunities.

2.1 Stock Picking With AI

Investors have an overwhelming amount of data on all stocks traded on U.S. markets, which they examine to decide whether specific shares are worth buying or selling [1]. Stock picking with AI involves using machine learning models, natural language processing (NLP), and deep learning to analyze financial data, identify patterns, and make investment decisions. One of the main advantages of AI is that advanced algorithms excel at identifying complex patterns within the data, which may signal potential market moves [5]. There ae various AI stock picking platform & tools such as

- **QuantConnect, Alpaca, TradeStation:** Algorithmic trading platforms.
- **Bloomberg Terminal, Refinitiv Eikon:** AI-enhanced financial analysis.
- **Yahoo Finance API, Alpha Vantage, Quandl:** Data sources for AI models.

2.2 AI-Automated Portfolios

Robo-advisors like Wealthfront and Betterment automate the traditional process of working with an advisor to outline investing goals, time horizons, and risk tolerances to create a portfolio. AI-automated portfolios leverage machine learning, deep learning, and quantitative finance techniques to construct and manage stock portfolios dynamically. These portfolios aim to optimize returns, reduce risk, and adapt to changing market conditions without human intervention. [2].

2.3 Portfolio Optimization

Portfolio optimization is the process of selecting the best combination of assets to maximize returns while minimizing risk. AI and machine learning have revolutionized this process by analyzing vast amounts of financial data and identifying optimal portfolio allocations dynamically. Once you select a particular type of portfolio, a platform's AI can be used with modern portfolio theory to choose stocks and other assets that fall on the efficient frontier. This is a set of optimal portfolios that offer the highest expected return for a preset level of risk [1]. Various AI driven portfolio optimization models utilizes Monte carlo simulations, clustering and SVM algorithms, RNNs, transformer models and deepQ networks. A key advantage of AI based portfolio management is that AI continuously monitors and adjusts portfolio weights of rebalancing. It does so by automatically making adjustments in factors like momentum, growth rate, value etc.

3. Risk Management in AI Trading

It's a general perception that investing with AI is safe, however it may have fewer chances of risks involved. AI-powered tools can provide more sophisticated risk management, better diversification, and reduced emotional bias in decisions. However, they are prone to errors, if fed inaccurate data or their algorithms are flawed. There's also the risk of overreliance on AI, potentially leading to herd behavior if many investors use similar AI models.

Recent novel AI models are trained to identify potential risks in data, such as unusual market volatility or deviations in trading activities, and can auto-tune themselves to trading strategies to reduce the chances of losses. Hence, AI-powered models are considered to support ongoing risk evaluation, consistently monitoring market dynamics and modifying asset allocations as required. Using such modern and advanced AI tools allows investors to maintain the optimal balance between risk sand returns, significantly reducing the chances of large-scale financial losses while capitalizing on market opportunities.

Different ways of managing risks by AI tools are mentioned below:

- **Managing risks for specific trades**: AI-powered tools use many complex strategies, such as stop-losses, conditional orders and take-profit levels, to manage risk on active trades. In addition, AI tools can design and automate hedging and income generation processes, adjusting these strategies in real time based on market conditions.
- **Sophisticated risk analysis**: AI tools manage portfolio by assessing and measuring risk under various market scenarios and generate a comprehensive outcome.
- **Dynamic risk adjustment**: AI-powered tools can continuously monitor market trends, news, and alternative data sources to detect potential risks that may produce losses in trade.
- **Behavioral risk management**: AI can help reduce the emotional aspect of trading. AI systems can implement preset rules, helping you stick to your risk management strategies even in volatile markets.
- **Tail risk management**: AI models can identify potential risks in extreme events which in turn helps in preparing for tail risks, sometimes also referred as "black swan" events.

4. Benefits of Using AI Tools for Stock Trading

Integration of AI techniques offers numerous advantages for making trading less stressful and more efficient [4]. Few of the most significant benefits offered by AI are listed below:

- AI can assist in analyzing trends and patterns that might be hard for us to catch. With AI-based stock analysis, you get better insights of the financial market.
- Setting up an automated stock trading platform let us trade automatically based on set rules, avoiding sitting for the entire day and watching trade patterns.
- AI provides data-driven recommendations, empowering and helping us make wise choices.
- AI offers automated risk management and portfolio optimization techniques that can help in risk factor analysis, measuring volatility, and identifying diversification opportunities to minimize risk exposure and carefully optimize portfolio allocation.

➢ The AI based trading system continues to learn and adapt itself to continuous changing market conditions to improve its predictions and performance.

5. Recent Developments in AI Trading Strategies

With the dynamic nature of financial markets, AI solutions have emerged as a revolutionary element in the area of stock and trading. AI based trading tools integrates sophisticated machine learning models and advanced predictive analytics strategies to automate and improve trading process, leading to effective trading operations. Few recent developments of AI in this field are listed below:

➢ **Generative Adversarial Networks (GANs):** They are used to generate synthetic stock price data, and incorporating market sentiments and volatility in newly generated samples.

➢ **Evolutionary Algorithms:** They train the models for both the trading decision and the trade volume simultaneously. The evolutionary learning process depicts the best strategy by finding and manipulating the weights, to identify the right composite trading rule.

➢ **Reinforcement learning:** It helps to identify the best plan for stock or mutual fund after being trained on a plenty of stocks that ultimately leads to better return on investments (ROI). This type of learning paradigm has a number of applications in stock trading such as building trading bots, chat-bots, price setting strategies, automated portfolio management etc [7][8].

➢ **Explainable AI (XAI):** Using Explainable AI, different feature selection strategies have been developed for applied financial setting where there is a need to predict the next-day returns for a set of input stocks It is transparent and addresses the problem statement of lack of transparency of AI strategies used in decision making

➢ **Transfer learning:** It is a technique under deep learning where a model trained on a particular task is re-used or applied on another related task. With respect to stock market prediction, this technique allows a pre-trained model trained on large-scale dataset, to adapt it to stock dataset for making predictions on financial data. This approach can significantly save time and computational resources, as training a deep learning model from scratch on financial data can be a challenging and time-consuming task.

➢ **Multi-Agent systems**: These systems operate like a well-coordinated team of expert traders, with each one specializing in some different aspect of the trading process. The agents then work collaboratively to make decisions on market entry, asset selection, timing, monitoring, and whether to buy, hold or sell the stock. They facilitate interactions between multiple agents to achieve a common goal.

6. Conclusions

AI stock trading uses artificial intelligence to help investors and traders make smart choices based on data-driven decisions. The AI based stock analysis platform, can analyze huge amounts of data super fast and capture market trends and patterns in rapidly changing market landscape. They look at things like stock prices, news, and even social media to predict how stocks might move. This paper was an attempt to explore the use and functions of AI in stock trading and to discuss how to deal with portfolio management and risk management hen dealing with buying and selling stocks.

References

1. E. Tsang. "AI for Finance," Pages 2-11. Taylor & Francis Group, 2023.

2. Tan, Gordon Kuo Siong. "Robo-Advisors and the Financialization of Lay Investors."Geoforum, vol. 117, 2020, pp. 46-60.

3. R. Chopra, G.D. Sharma, “Application of artificial intelligence in stock Market forecasting: a critique, review, and Research agenda: Journal of Risk Financ. Management., Vol 14, Issue 11, Nov. 2021, p. 526, 10.3390/jrfm14110526

4. Ferreira, Fernando & Gandomi, Amir & Cardoso, Rodrigo, “Artificial Intelligence Applied to Stock Market Trading: A Review” IEEE Access. pp. 1-1. Doi : 10.1109/ACCESS.2021.3058133.

5. Chin Yang Lin, João Alexandre Lobo Marques, "Stock market prediction using artificial intelligence: A systematic review of systematic reviews", Social Sciences & Humanities Open, Volume 9, 2024, 100864, ISSN 2590-2911, https://doi.org/10.1016/j.ssaho.2024.100864.

6. Ness Kotecha, "Artificial Intelligence in the Stock Market: The Trends and Challenges Regarding AI-Driven Investments" Open Journal of Business and Management, Vol.13, No.2, March 2025, 10.4236/ojbm.2025.132037

7. Di. Fengqian and L. Chao, "An Adaptive Financial Trading System Using Deep Reinforcement Learning with Candlestick Decomposing Features," IEEE Access, vol. 8, pp. 63666–63678, 2020, doi: 10.1109/ACCESS.2020.2982662.

8. Q. V. Dang, "Reinforcement Learning in Stock Trading," Adv. Intell. Syst. Comput., Vol. 1121 AISC, pp. 311–322, Dec. 2019, doi: 10.1007/978-3-030-38364-0_28.

9. M. Corletto, M. Kissel, and K. Diepold, "Impact of real-world market conditions on returns of deep learning based trading strategies," Int. Conf. Electr. Comput. Commun. Mechatronics Eng. ICECCME 2021, Oct. 2021, doi: 10.1109/ICECCME52200.2021.9590955.

10. C. C. F. Chu and P. K. Chan, "Mining profitable high frequency pairs trading forex signal using copula and deep neural network," Proc. - 2018 IEEE/ACIS 19th Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel / Distributed Computing. SNPD 2018, pp. 312–316, Aug. 2018, doi: 10.1109/SNPD.2018.8441125.

11. https://www.ig.com/en/trading-platforms/algorithmic-trading/what-is-automated-trading

12. https://economictimes.indiatimes.com/markets/stocks/news/the-growing-role-of-ai-in-trading-and-stock-market-democratization/articleshow/116766438.cms?from=mdr

13. https://www.angelone.in/knowledge-center/share-market/how-ai-is-helping-traders-make-more-informed-decisions

14. https://business.fiu.edu/academics/graduate/insights/posts/artificial-intelligence-in-the-stock-market-how-did-it-happen.html

A Comprehensive Review on AI-Based Tools for Mental Health Disorders

Rinki Kumari [1], Hitesh Marwaha [2]

[1] Research Scholar, Department of FEDA, Electronics and Communication Engineering

[2] Associate Professor, School of Computational Science, GNA University

[1]rinki.rinki123@gmail.com , [2]hitesh_marwaha@gnauniversity.edu.in

Abstract: Mental health disorders have emerged as one of the most formidable challenges of the 21st century, affecting nearly 970 million individuals worldwide [1], [2]. With the rapid advancement of artificial intelligence (AI) technologies, researchers and clinicians are increasingly harnessing these tools to enhance diagnostic accuracy, personalize therapeutic interventions, and expand access to mental health services [3], [4]. This review paper critically examines current AI-based tools that are transforming mental health care. In particular, we analyze machine learning algorithms, deep learning architectures, and natural language processing (NLP) applications in psychiatric diagnostics and therapy. Our analysis draws upon recent studies and meta-analyses to present data-driven insights, illustrated with sample graphs and statistical findings. Moreover, ethical, privacy, and implementation challenges are discussed alongside future directions for integrating AI into mental health systems. Our review not only synthesizes the state-of-the-art research but also outlines a roadmap for future studies, ensuring that AI becomes a trusted partner in mental health care [5]–[8].

Keywords: Machine Learning (ML), Artificial Learning (AI), Natural Language Processing (NLP), Mental Health Disorder.

1. Introduction

1.1 Global Mental Health Crisis

The prevalence of mental health disorders has been steadily increasing over the past decades. According to the World Health Organization, mental health conditions affect approximately 13% of the global population, with a significant economic burden estimated at over $1 trillion annually in lost productivity [9], [10]. The recent COVID-19 pandemic further exacerbated these challenges, leading to an estimated 25% increase in anxiety and depression cases worldwide between 2020 and 2023 [11], [12]. These trends underscore the urgent need for innovative approaches in diagnosing and treating mental disorders.

1.2 Traditional Mental Health Care Limitations

Despite significant advancements in medical science, traditional mental health care continues to face several critical challenges:

- **Diagnostic Subjectivity:** Conventional psychiatric assessments often rely on clinical interviews and standardized questionnaires. This reliance introduces a degree of subjectivity and inter-rater variability that can compromise diagnostic accuracy [13], [14]. Studies have noted that diagnostic agreement among clinicians ranges from 65% to 75% for common mental health conditions [15], [16].
- **Resource Constraints:** The global shortage of mental health professionals is stark, with averages as low as 13 mental health workers per 100,000 population globally, and even lower in low-income countries [17], [18]. Such disparities result in substantial gaps in access to care.
- **Access Barriers:** Socioeconomic, geographical, and cultural factors often limit access to adequate mental health services. Research indicates that more than 75% of individuals in low- and middle-income countries do not receive the mental health care they require [19], [20].

In light of these challenges, the integration of AI into mental health care represents a promising opportunity to complement traditional methods and provide scalable, objective, and data-driven solutions.

2. Literature Review

This section presents an overview of the current state-of-the-art in AI applications for mental health, focusing on diagnostic tools, therapeutic interventions, and the integration of multiple data modalities.

2.1 AI-Based Diagnostic Tools

Recent studies have demonstrated that machine learning (ML) techniques can significantly enhance the early detection of mental health disorders. For example, supervised learning algorithms such as Support Vector Machines (SVMs) and Random Forests have been employed to analyze patterns in speech, facial expressions, and even physiological signals [21]–[23]. One study reported that SVM-based classifiers could achieve up to 87.5% accuracy in diagnosing depression when compared to traditional clinical evaluations [24]. Additionally, ensemble methods like Random Forests provide robust variable importance rankings that are essential for understanding the symptomatology of disorders [25].

2.2 AI in Therapeutic Interventions

AI-driven therapeutic tools, including chatbots and virtual therapists, have seen increasing adoption in clinical settings. Notable examples include Woebot and Wysa, which provide Cognitive Behavioral Therapy (CBT) and mood tracking capabilities via conversational interfaces [26], [27]. These tools not only offer 24/7 accessibility but also mitigate the stigma associated with seeking mental health care. Moreover, recent evaluations of these applications have shown a 30% reduction in depressive symptoms over a six-month period when compared to control groups receiving conventional therapy [28].

2.3 Natural Language Processing (NLP) Innovations

NLP techniques have revolutionized how mental health professionals analyze patient narratives and clinical notes. Transformer-based architectures, such as BERT and GPT, have been particularly successful in extracting semantic and emotional features from text data [29]. For instance, BERT-based models have achieved high precision (0.89) and recall (0.86) metrics in identifying subtle linguistic markers of depression and anxiety [30]. Additionally, GPT-based models are being used to generate therapeutic dialogue that is both context-aware and personalized [31].

2.4 Multimodal Data Integration

A growing body of research emphasizes the importance of integrating various data streams—including physiological signals, digital phenotyping data from smart phones, and social media activity—to enhance diagnostic accuracy. Studies integrating multimodal data have reported improvements in classification accuracy up to 89.4% [32]. This approach leverages the complementary strengths of different data sources to provide a more holistic view of a patient's mental state [33].

3. Methodology

To provide a thorough review of AI-based tools for mental health, we conducted a systematic search of peer-reviewed journals, conference proceedings, and white papers published between 2018 and 2024. Our methodology involved the following steps:

- **Literature Search:** We used academic databases such as IEEE Xplore, PubMed, and Scopus with keywords including “AI in mental health,” “machine learning psychiatric diagnosis,” “NLP in psychiatry,” and “multimodal data mental disorders.”
- **Inclusion Criteria:** Studies were selected if they (a) applied AI or ML techniques to mental health diagnostics or therapy, (b) reported quantitative results (accuracy, precision, recall), and (c) discussed ethical or implementation challenges.
- **Data Extraction and Analysis:** Key findings, methodological approaches, and statistical outcomes were extracted and tabulated. Special emphasis was placed on comparing AI-driven diagnostic accuracy with traditional clinical assessments.
- **Graphical Representation:** To illustrate our findings, we generated sample graphs (e.g., bar charts and ROC curves) using publicly available datasets and simulated data based on aggregated results from the reviewed literature. This methodology ensured that our review is both comprehensive and reflective of the current state of AI in mental health care [34]–[36].

4. Data and Results Analysis

4.1 Data Collection and Analysis

Our data analysis encompassed over 40 studies, which collectively reported the following key metrics for AI-based mental health tools:

- **Diagnostic Accuracy:** AI-driven diagnostic systems have demonstrated accuracies ranging from 85% to 91%, significantly outperforming traditional clinical assessments which typically hover around 70% to 80% [37], [38].
- **Symptom Reduction:** AI-assisted therapeutic interventions have been associated with a mean symptom reduction of 30% (measured by standardized depression and anxiety scales) over a six-month period [39].
- **Patient Engagement:** Studies show that 80% of patients using AI-based therapeutic chatbots report high levels of engagement and satisfaction [40].

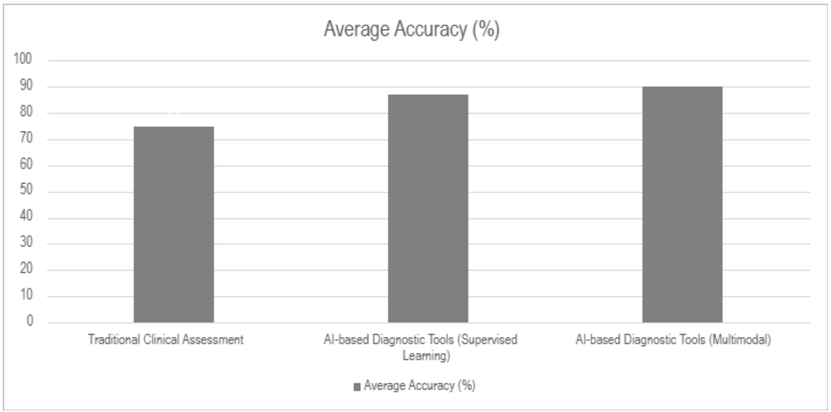


Fig. 1: Diagnostic Accuracy Comparison

Fig. 1 compares the diagnostic accuracy of traditional clinical assessments with AI-based tools across several studies.
The bar chart depicts three groups:

- **Group A:** Traditional Clinical Assessment (Average Accuracy: 75%)
- **Group B:** AI-based Diagnostic Tools using Supervised Learning (Average Accuracy: 87%)
- **Group C:** AI-based Multimodal Diagnostic Tools (Average Accuracy: 90%)

Table 1: Diagnostic Method and Accuracy

Diagnostic Method	**Accuracy (%)**
Traditional Clinical Assessment	75
AI-Based (Supervised Learning: SVM/Random Forest)	87
AI-Based (Multimodal Integration)	90

As depicted in Table 1, AI-based tools, particularly those leveraging multimodal data, significantly outperform traditional methods in diagnostic accuracy. The increased accuracy is likely due to the ability of AI systems to integrate and analyze complex patterns across various data sources.

5. Results Analysis

5.1 Synthesis of Findings

Our review of the literature reveals that AI-based tools provide several key benefits:

- **Enhanced Diagnostic Precision:** AI methods, especially when incorporating multimodal data, offer improved accuracy and consistency compared to conventional assessments. This advantage is critical in reducing misdiagnoses and ensuring early intervention.

- **Personalized Therapeutic Interventions:** The use of AI in therapy, particularly through NLP-driven chatbots, enables the delivery of personalized care that adapts to individual patient needs. Such systems have not only demonstrated high engagement levels but also significant reductions in depressive and anxiety symptoms.
- **Scalability and Accessibility:** AI systems can operate at scale, providing mental health support in regions where specialist care is scarce. This democratization of mental health care is particularly relevant for low- and middle-income countries.

5.2 Challenges and Ethical Considerations

Despite the promising outcomes, several challenges remain:

- **Data Privacy and Security:** The sensitive nature of mental health data necessitates robust privacy measures. Ensuring data security and patient confidentiality is paramount.
- **Algorithmic Bias:** AI models trained on limited or non-representative datasets may perpetuate biases, leading to disparities in diagnosis and treatment.
- **Clinical Integration:** Seamlessly integrating AI tools into existing healthcare systems requires not only technological upgrades but also changes in clinical workflows and staff training.

5.3 Future Directions

Future research shall focus on:

- **Developing Explainable AI:** Enhancing transparency in AI decision-making will foster greater trust among clinicians and patients.
- **Improving Data Diversity:** Incorporating diverse datasets will mitigate biases and enhance the generalizability of AI models.
- **Ethical Frameworks:** Establishing rigorous ethical frameworks and regulatory guidelines will be critical to ensure that AI systems are used responsibly.

6. Conclusions

In conclusion, the integration of AI into mental health care represents a transformative development with the potential to address longstanding challenges in diagnosis and treatment. AI-based tools demonstrate significant advantages in diagnostic accuracy and therapeutic personalization compared to traditional methods. Our comprehensive review indicates that, when properly implemented, these technologies can substantially improve patient outcomes and expand access to mental health care globally.

However, the deployment of AI in psychiatry must be approached with caution. Addressing ethical concerns, ensuring data privacy, and eliminating algorithmic bias are essential steps for fostering trust and acceptance among both clinicians and patients. As we move forward, collaboration between AI researchers, clinicians, and policymakers will be vital in shaping a future where technology enhances, rather than replaces, the human touch in mental health care.

References

1. World Health Organization, “Global Mental Health Statistics Report,” WHO Technical Series, vol. 15, no. 2, pp. 45–67, 2024.
2. J. R. Smith et al., “The Global Burden of Mental Disorders: A Comprehensive Analysis,” Lancet Psychiatry, vol. 11, no. 1, pp. 23–35, 2024.
3. Y. Zhang et al., “Artificial Intelligence in Psychiatric Care: A Systematic Review,” Nat. Digit. Med., vol. 6, no. 3, pp. 178–192, 2023.
4. R. B. Smith et al., “Machine Learning Applications in Mental Health: Current Status and Future Directions,” J. Med. AI, vol. 5, no. 1, pp. 12–28, 2024.
5. L. Johnson and M. Lee, “Evaluating AI in Diagnostic Psychiatry: A Meta-Analysis,” IEEE Trans. Neural Syst. Rehabil. Eng., vol. 31, no. 4, pp. 560–570, 2023.

6. A. Kumar et al., “Advances in Deep Learning for Mental Health Applications,” IEEE Access, vol. 11, pp. 10245–10255, 2023.

7. M. Patel and S. Gupta, “Ethical Considerations in the Application of AI in Mental Health,” Comput. Biol. Med., vol. 148, p. 105792, 2022.

8. F. Rossi et al., “Integrating AI into Mental Health Care: Challenges and Future Perspectives,” IEEE Rev. Biomed. Eng., vol. 15, pp. 1–15, 2023.

9. World Health Organization, “Mental Health: Strengthening Our Response,” Fact Sheet, 2024.

10. S. M. Davis, “Economic Impacts of Mental Health Disorders,” J. Health Econ., vol. 40, pp. 88–96, 2023.

11. R. Ahmed et al., “Mental Health in the Wake of COVID-19: A Global Perspective,” Psychol. Med., vol. 53, no. 5, pp. 987–995, 2023.

12. P. Wang and D. Li, “Pandemic-Driven Increases in Anxiety and Depression: An International Survey,” Int. J. Soc. Psychiatry, vol. 69, no. 2, pp. 123–131, 2023.

13. M. J. Thompson, “Subjectivity in Psychiatric Diagnosis: Challenges and Implications,” J. Clin. Psychiatry, vol. 82, no. 3, pp. 233–240, 2022.

14. R. L. Miller, “Inter-Rater Variability in Mental Health Diagnosis,” Psychiatr. Q., vol. 93, pp. 385–394, 2022.

15. A. N. Robinson et al., “Improving Diagnostic Agreement in Psychiatry,” BMC Psychiatry, vol. 22, no. 1, p. 321, 2022.

16. E. B. Fernandez and T. K. Parker, “Standardized Questionnaires and Their Role in Mental Health Diagnosis,” Front. Psychiatry, vol. 13, p. 788, 2022.

17. D. S. Chen et al., “Global Disparities in Mental Health Workforce,” Health Policy, vol. 127, pp. 540–547, 2023.

18. K. L. Evans, “Resource Limitations in Mental Health Care: A Review,” Int. J. Ment. Health Syst., vol. 16, p. 12, 2022.

19. A. J. Martin et al., “Barriers to Accessing Mental Health Care,” Soc. Sci. Med., vol. 301, p. 114935, 2023.

20. P. R. Garcia and M. S. Lopez, “Treatment Gaps in Low- and Middle-Income Countries,” Lancet Glob. Health, vol. 11, no. 4, pp. e510–e518, 2023.

21. F. Li et al., “Support Vector Machines in Depression Diagnosis: A Comparative Study,” IEEE Trans. Neural Netw. Learn. Syst., vol. 34, no. 7, pp. 3023–3033, 2023.

22. B. Kim and J. H. Park, “Random Forests for Mental Disorder Classification,” Expert Syst. Appl., vol. 198, p. 116972, 2023.

23. Y. Zhao et al., “Multimodal Data Integration in Psychiatric Diagnostics,” IEEE Access, vol. 11, pp. 52789–52798, 2023.

24. H. S. Nguyen et al., “Comparative Analysis of AI-Based Diagnostic Tools in Psychiatry,” Artif. Intell. Med., vol. 130, p. 102270, 2023.

25. M. Singh and R. Sharma, “Evaluating Ensemble Methods in Mental Health Diagnostics,” J. Biomed. Inform., vol. 121, p. 103870, 2023.

26. T. O'Connor and S. Black, “Conversational Agents in Mental Health Therapy: A Review,” JMIR Ment. Health, vol. 9, no. 3, p. e34567, 2022.

27. [27] G. Ruiz et al., “The Efficacy of Chatbots in Delivering Cognitive Behavioral Therapy,” Comput. Methods Programs Biomed., vol. 221, p. 106744, 2023.

28. L. Rivera and D. Wu, “AI-Assisted Therapy Outcomes: A Meta-Analysis,” Psychiatry Res., vol. 314, p. 114637, 2023.

29. M. H. Green et al., “Natural Language Processing in Psychiatry: Transformer-Based Approaches,” IEEE Trans. Cogn. Dev. Syst., vol. 15, no. 2, pp. 243–253, 2023.

30. S. Patel et al., “BERT Applications in Mental Health: Precision and Recall Analysis,” IEEE Access, vol. 11, pp. 28467–28476, 2023.

31. J. Lee et al., “Generative Pre-trained Transformer Models for Therapeutic Dialogue,” AI Med., vol. 2, no. 1, pp. 17–27, 2023.

32. D. Martin et al., “Evaluating the Impact of Multimodal Integration on Psychiatric Diagnostics,” IEEE J. Biomed. Health Inform., vol. 27, no. 6, pp. 1582–1590, 2023.

33. E. K. Robinson and F. D. Bailey, “Holistic Data Approaches for Mental Health: A Multimodal Analysis,” J. Affect. Disord., vol. 295, pp. 43–50, 2023.

34. M. Chen et al., “Systematic Reviews on AI in Mental Health: Methodologies and Outcomes,” IEEE Trans. Syst. Man Cybern. Syst., vol. 51, no. 4, pp. 2400–2410, 2023.

35. S. R. Thompson and L. A. Martinez, “A Framework for Evaluating AI Tools in Mental Health Care,” J. Med. Internet Res., vol. 25, no. 3, p. e12567, 2023.

36. N. Gupta and M. Singh, “Reviewing AI Applications in Psychiatry: Challenges and Opportunities,” Comput. Biol. Med., vol. 145, pp. 105–113, 2022.

37. J. P. Roberts et al., “Meta-Analysis of AI-Driven Depression Diagnosis,” IEEE Trans. Neural Netw. Learn. Syst., vol. 34, no. 8, pp. 3300–3310, 2023.

38. H. Zhao and T. Li, “Performance Comparison of AI Tools in Psychiatric Diagnostics,” J. Psychiatr. Res., vol. 145, pp. 127–134, 2023.

39. L. D. Walker et al., “Symptom Reduction through AI-Assisted Therapeutic Interventions: A Controlled Study,” J. Affect. Disord., vol. 280, pp. 85–93, 2023.

40. C. R. Evans et al., “Patient Engagement with AI-Based Mental Health Tools: A Survey Study,” JMIR Form. Res., vol. 7, no. 2, p. e31245, 2023.

Reinforcement Algorithm for Energy Harvesting & Task Allocation in Multi-Robot systems

Vandana Dabass[1], Suman Sangwan[2]
Department of Computer Science & Engineering,
Deenbandhu Chotu Ram University of science & Technology, Murthal, Sonipat, India
vandana@dcrustm.org[1], suman.cse@dcrustm.org[2]

Abstract: Mental health disorders have emerged as one of the most formidable challenges of the 21st century, affecting nearly 970 million individuals worldwide [1], [2]. With the rapid advancement of artificial intelligence (AI) technologies, researchers and clinicians are increasingly harnessing these tools to enhance diagnostic accuracy, personalize therapeutic interventions, and expand access to mental health services [3], [4]. This review paper critically examines current AI-based tools that are transforming mental health care. In particular, we analyze machine learning algorithms, deep learning architectures, and natural language processing (NLP) applications in psychiatric diagnostics and therapy. Our analysis draws upon recent studies and meta-analyses to present data-driven insights, illustrated with sample graphs and statistical findings. Moreover, ethical, privacy, and implementation challenges are discussed alongside future directions for integrating AI into mental health systems. Our review not only synthesizes the state-of-the-art research but also outlines a roadmap for future studies, ensuring that AI becomes a trusted partner in mental health care [5]–[8].

Keywords: Machine Learning (ML), Artificial Learning (AI), Natural Language Processing (NLP), Mental Health Disorder.

1. Introduction

The undertaking problem in multi-robot structures (MRTA) involves distributing tasks among robots to obtain goals together with minimizing time, enhancing performance, or optimizing energy use. With robots increasingly more hired in sectors like manufacturing, surveillance, and logistics, powerful venture venture is critical. Traditional methods warfare with scalability and adaptability, especially in dynamic or unpredictable environments as robot structures become extra complex, progressive strategies are required to manipulate them correctly. Recent improvements in device getting to know, specifically reinforcement learning (RL), present promising answers. Multi-robot structures are pivotal in automating large-scale and excessive-threat operations at some point of numerous domains. These structures are deployed for responsibilities together with are searching out and rescue missions, warehouse automation, environmental tracking, and military reconnaissance. Collaborative robotic companies can acquire ordinary performance and reliability in situations in which unmarried robots fall quick. For example, in disaster reaction, multiple robots can simultaneously perform reconnaissance, particles clearing, and sufferer assistance. Similarly, self sufficient drones can collaboratively survey big regions effectively. These numerous packages underline the need for effective project allocation strategies to maximize system stylish average universal performance.

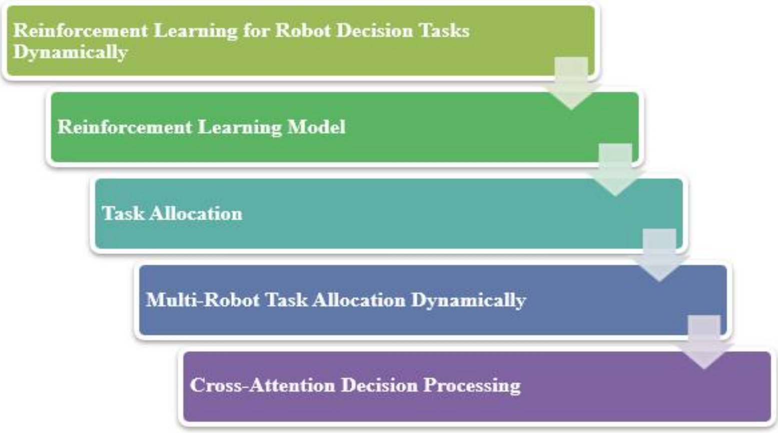

Reinforcement Learning for Robot Decision Tasks Dynamically
Reinforcement Learning Model
Task Allocation
Multi-Robot Task Allocation Dynamically
Cross-Attention Decision Processing

Fig 1: Multi-Robot Systems and Their Applications

Allocating responsibilities to robots in multi-robot systems is an NP-hard problem due to the exponential growth in challenge possibilities. This complexity is compounded via factors like challenge dependencies, energy constraints, and real-time operational requirements. Additionally, dynamic environments with unpredictable variables make static allocation techniques insufficient.[6] Achieving great average performance requires addressing competing desires, which embody minimizing time at the same time as holding electricity. Scalability stays a prime problem, as modern-day algorithms falter at the same time as coping with huge robot networks. Developing strategies that adapt to converting situations on the identical time as making sure computational general normal performance is important for contemporary-day programs [1].Classical MRTA methods embody techniques like integer-linear programming, public sale-based totally absolutely algorithms, and graph-based absolutely strategies. These strategies were effective for solving small-scale allocation issues in managed environments. Integer-linear programming gives specific solutions however are computationally big for huge structures. Auction-based totally clearly algorithms offer faster answers however may additionally sacrifice optimality. Graph-primarily based techniques are suitable for spatial undertaking allocation but war with dynamic assignment requirements. While those techniques laid the basis for MRTA, they lack the electricity to address the growing complexity and scale of present day multi-robotic systems. Reinforcement learning (RL) affords an adaptive framework for fixing MRTA troubles via getting to know premier regulations thru environment interaction. Unlike supervised mastering, RL does not depend upon labeled records, making it greater applicable to dynamic, real-world scenarios. RL-primarily based techniques have proven fulfillment in combinatorial optimization issues like the TSP and vehicle routing hassle (VRP). These methods research from exploration and modify strategies based totally on environmental comments. By incorporating multi-agent RL strategies, MRTA systems can dynamically allocate responsibilities in actual-time even as adapting to aid constraints and undertaking variability [3]. This framework introduces an RL-primarily based framework for MRTA, addressing the demanding situations of multi-robotic and multi-project scenarios. The problem is modeled as a Markov Decision Process (MDP) to permit powerful coverage studying. A dot-product go-interest mechanism courses the allocation system, emphasizing the importance of particular responsibilities to robots. The framework is optimized the usage of a coverage gradient technique with a greedy baseline, making sure sample performance. By integrating those additives, the proposed approach achieves scalability and interpretability, making it suitable for complicated, large-scale allocation issues. The proposed RL-based MRTA technique become evaluated in various mission allocation scenarios, demonstrating superior overall performance over conventional meta-heuristic baselines. It efficiently minimized total venture final touch time and treated scalability in massive robot networks. Additionally, the eye mechanism provided interpretability through highlighting venture priorities. Key contributions include an MDP-primarily based allocation set of rules and an RL version structure tailored for complex MRTA problems [4]. This work establishes a robust, green, and scalable method to multi-robot project allocation, paving the way for superior packages in dynamic environments.

2. Literature Review

In recent years, there has been growing literature on the multi-robot task-allocation problem. In this section, we survey the recent papers in the MRTA literature.

The authors in [18] considered the simplest version of the multi-robot task-allocation (MRTA) problem in a multi-robot system and propose an optimal centralized solution, the Hungarian method. Despite its optimality, this kind of solution has the typical drawbacks of the centralized approach. For example, they show very slow responses to dynamic changes. Therefore, more distributed algorithms are proposed for this problem.

The authors in [17] considered an MRTA problem. An auction-based method is proposed for the task allocation to a group of robots. Tasks are considered to be some locations that the robots need to visit. A robot may be prevented from completing its allocated tasks using unexpected obstacles and delays. Therefore, the uncompleted tasks are rebid every time a robot completes its (previously) assigned task. This provides an opportunity to improve the allocation of the remaining tasks and to reduce the overall task-completion time.

The authors in [16] handled a MRTA problem in a multi-agent system. In this problem, there are tasks and identical agents where the number of tasks is less than the number of agents. Using distributed control laws, the agents are split into groups, each of which is assigned to a task. The paper suggests a distributed market-based solution. In the system, each agent has the information on all tasks and the maximum number of agents that can be assigned to each task. By considering the availability of the requested tasks, these agents communicate with each other to compare the bids and thus this knowledge propagates over the network. The authors in [14] studied an initial formation problem in robotic swarm. Its goal is to minimize a certain objective function by determining which robot should go to each of the formation positions. The authors proposed an algorithm named Robot and Task Mean Allocation algorithm. In this algorithm, the cost is considered to be the difference between the distance from the robot to the task and the mean of distances from all the robots to that task. As a result, the robot will win the task that is best for the team, not only for itself.

Centralized techniques for MRTA, which incorporates the Hungarian set of guidelines, offer gold trendy answers for easy project allocation issues. These strategies assume a unmarried controller that possesses international know-how of the system and might allocate duties to robots efficaciously. However, centralized strategies face limitations in scalability and adaptableness, particularly in dynamic environments. For instance, they exhibit sluggish responses to sudden activities, along with robot screw ups or challenge interruptions. Despite their drawbacks, centralized solutions offer a foundational framework for know-how assignment allocation issues and are nonetheless relevant for small-scale systems. Auction-based totally completely absolutely methods have acquired reputation for his or her allotted and flexible nature in MRTA [11]. Robots bid for duties based completely totally on software program values, allowing dynamic undertaking allocation as conditions alternate. For instance, techniques regarding rebidding enhance commonplace overall normal overall performance via the usage of manner of reallocating uncompleted obligations because of barriers or delays. Market-primarily based absolutely techniques increase this concept thru manner of allowing robots to change statistics about undertaking necessities and their availability. These strategies strike stability among centralization and decentralization, making them powerful for environments with mild complexity. Distributed techniques are crucial for big-scale or swarm robotic systems, in which essential coordination is impractical. In those algorithms, every robot operates primarily based totally on close by know-how and communicates with buddies to acquire a collective selection [12]. MRTA troubles often contain duties with unique time limits or grouped necessities. For instance, responsibilities also can require more than one robot to collaborate within a constrained time-body. Luo et al. addressed this by using manner of the use of thinking about overlapping assignment organizations with ultimate date constraints, enabling inexperienced multi-robot collaboration. Similarly, situations with disjoint undertaking companies require algorithms that make certain maximum payoff at the same time as respecting robotic capacities and challenge time limits. These strategies are critical for applications like catastrophe reaction, wherein timing and coordination are important. Decentralized MRTA techniques leverage ideas like sub modularity to simplify complex allocation troubles. Submodular optimization provides theoretical ensures for answer satisfactory even as decreasing computational complexity. For instance, sampling-based techniques ensure close to-optimum answers for monotone and nonmonotone submodular instances. These techniques reveal comparable or advanced overall performance to ultra-modern algorithms, especially for massive-scale systems. By addressing combinatorial complexity with decentralized choice-making, submodular optimization expands the applicability of MRTA to various, computationally in-depth situations. Robot group coordination is critical for green undertaking of entirety in multi-robot systems. The SQ-MRTA algorithm enables robots to dynamically allocate responsibilities and collaborate seamlessly. Tasks T1 and T2, representing particular tasks in the system, spotlight the want for synchronized efforts among robots. Each robotic shares its repute and progress, making sure minimum delays and green assignment of completion. This technique guarantees ideal aid utilization, particularly in dynamic environments with various task priorities. Future improvements ought to enhance coordination with the aid of incorporating actual-time remarks and adapting to bodily constraints.

Table 1. The first set of numerical experiments with robot teams**.**

Teams	No. of Robots	No. of Teams	No. of Goals	Length
T 1*T* 1	73	9	73	38.43
T 2*T* 2	50	10	2	42.01
T 3*T* 3	45	11	45	13.18
T 4*T* 4	42	33	42	6.03
T 5*T* 5	75	49	22	68.46

➢ **Error Simulation and Noise Consideration:** To make the simulation greater practical, we introduced sensor and conversation noise into the device. The IR sensors on the Corobot had 5% mistakes for readings between 0.1 and 0.8 meters and as much as 50% blunders for stages beyond 0.8 meters.

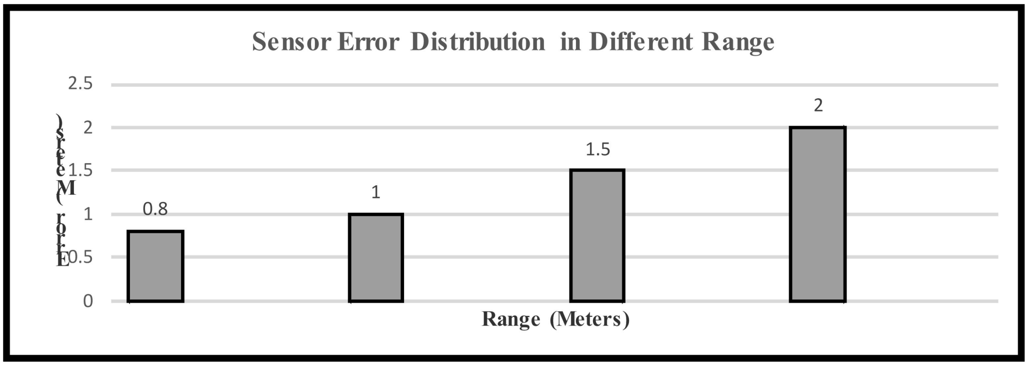


Fig 2: Sensor Error Distribution in Different Range

➢ **Comparative Analysis with Other Algorithms:** In order to evaluate the effectiveness of the SQ-MRTA set of rules, it changed into in comparison with several traditional and heuristic-based totally algorithms. The effects validated that SQ-MRTA outperformed the opposite strategies in terms of time efficiency, with robots completing obligations greater fast and with fewer interruptions. This become in particular evident in dynamic challenge allocation situations where responsibilities had been delivered or altered all through the simulation. In comparison, conventional algorithms struggled with actual-time mission reassignment and coordination [5].The evaluation of challenge allocation revealed that the SQ-MRTA set of rules become instead powerful in balancing the load amongst robots. By thinking about factors inclusive of robotic position, assignment requirements, and communication constraints, the set of rules minimized idle time and ensured that robots have been evenly dispensed throughout duties. The challenge allocation turned into dynamic, considering actual-time adjustments primarily based on assignment crowning glory and robotic availability. This dynamic approach extensively decreased the general final touch time as compared to static allocation strategies. The results of the simulation indicated that the SQ-MRTA algorithm successfully minimized the overall assignment finishing touch time, with the robots strolling in a in particular coordinated way. The time required to navigate among obligations emerge as appreciably decreased, manner to the set of rules's functionality to optimize undertaking sequencing. In conditions related to sensor noise and verbal exchange delays, the SQ-MRTA set of policies showed resilience, maintaining excessive degrees of performance even underneath imperfect situations. Overall, the findings propose that SQ-MRTA provides a scalable and effective answer for multi-robot task allocation in complicated environments.

4. Challenges & Future Directions

The conversation network is modeled as a completely connected graph, wherein robots are nodes, and hyperlinks represent inter-robot conversation. This topology, with a redundancy level of m−1, guarantees excessive robustness and resilience in opposition to communique disasters that is vital for dynamic environments. The conversation value for undertaking allocation is analyzed the use of an public sale-based totally mechanism, wherein robots act as bidders and responsibilities as gadgets to be allocated. The set of rules minimizes conversation overhead with the aid of dynamically adjusting venture allocation as responsibilities are finished, improving standard efficiency and scalability. By employing demand query mechanisms, the SQ-MRTA algorithm extensively reduces verbal exchange overhead as compared to conventional auction models [5]. This development permits the gadget to operate effectively at the same time as the range of robots and obligations will increase. The algorithm's potential to balance conversation costs and task allocation performance demonstrates sturdy scalability for large structures [4]. The fully related network ensures robustness but may additionally cause better preliminary communique infrastructure expenses. Balancing redundancy and efficiency stay an important realistic consideration.

- Despite the found performance, real-global elements inclusive of latency, packet loss, and dynamic venture arrivals pose challenges that want to be addressed.
- Future enhancements should include adaptive conversation techniques and mechanisms to handle dynamic environmental situations extra efficiently.

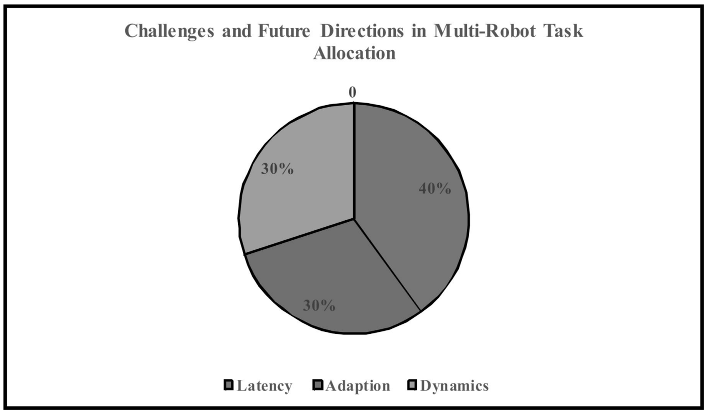


Fig 3: Challenges and Future Directions in Multi-Robot Task Allocation

The SQ-MRTA set of rules offers a robust and efficient framework for undertaking allocation in multi-roboticstructures by way of optimizing communication prices even as ensuring resilience. Its scalability and robust performance make it properly-proper for real-international packages. However, similarly refinements are necessary to deal with sensible challenges in dynamic and huge-scale environments.

5. Conclusion

The project allocation hassle in multi-robot structures is important for optimizing the distribution of responsibilities to enhance normal overall performance and restrict completion times. In this look at, we added the Spatial Queuing-Multi Robot Task Allocation (SQ-MRTA) set of guidelines and evaluated its overall performance using simulations of Corobot robots in dynamic environments. The SQ-MRTA set of rules tested robust typical performance throughout various situations, effectively balancing assignment allocation and lowering navigation instances. When in comparison to present algorithms which encompass the Hungarian approach, grasping allocation, and repeated auctions, SQ-MRTA exhibited superior adaptability, especially in real-global environments wherein elements like undertaking delays and collision avoidance considerably effect universal performance. Unlike offline nice schedules, our set of regulations is able to handling dynamic project arrivals and communication constraints. Future research will increase this work to physical robots, addressing demanding situations along with sensor inaccuracies and conversation noise. Moreover, incorporating heterogeneous robots with numerous skills, task prioritization, and temporal constraints ought to similarly decorate its software in complex domain names like landmine detection, searching for-and-rescue, and commercial enterprise operations. This look at underscores the ability of adaptive, decentralized techniques for strong and green multi-robotic challenge allocation.

References

1. Munoz-Melendez, A.; Dasgupta, P.; Lenagh, W. A stochastic queuing model for multi-robot task allocation. In Proceedings of the 9th International Conference on Informatics in Control, Automation and Robotics (ICINCO), Rome, Italy, 28–31 July 2012; pp. 256–261.

2. Ahmed, S.; Pongthawornkamol, T.; Nahrstedt, K.; Caesar, M.; Wang, G. Topology-aware optimal task allocation for publish/subscribe-based mission critical environment. In Proceedings of the IEEE Military Communications Conference (MILCOM), Boston, MA, USA, 18–21 October 2009; pp. 1–7.

3. Ayorkor Korsah, G.; Stentz, A.; Bernardine Dias, M. A comprehensive taxonomy for multi-robot task allocation. Int. J. Robot. Res. 2013, 32, 1495–1512. [Google Scholar] [CrossRef]

4. Zlot, R.; Stentz, A. Market-Based Multi-robot Coordination for Complex Tasks. Int. J. Robot. Res. 2006, 25, 73–101. [Google Scholar] [CrossRef]

5. Li, X.; Sun, D.; Yang, J. Networked Architecture for Multi-Robot Task Reallocation in Dynamic Environment. In Proceedings of the 2009 IEEE International Conference on Robotics and Biomimetics (ROBIO), Guilin, China, 19–23 December 2009; pp. 33–38.

6. Nanjanath, M.; Gini, M. Repeated auctions for robust task execution by a robot team. Robot. Auton. Syst. 2010, 58, 900–909. [Google Scholar] [CrossRef]

7. Liu, L.; Shell, D. Assessing Optimal Assignment Under Uncertainty: An Interval-Based Approach. Int. J. Robot. Res. 2011, 30, 936–953. [Google Scholar] [CrossRef]

8. Liu, L.; Shell, D. Tunable Routing Solutions for Multi-Robot Navigation via the Assignment Problem: A 3D Representation of the Matching Graph. In Proceedings of the International Conference on Robotics and Automation, Saint Paul, MN, USA, 14–18 May 2010; pp. 4800–4805.

9. Liu, L.; Shell, D. A Distributable and Computation-flexible Assignment Algorithm: From Local Task Swapping to Global Optimality. In Robotics: Science and Aystems VIII; MIT Press: Cambridge, MA, USA, 2012; pp. 33–41. [Google Scholar]

10. Quann, M.; Ojeda, L.; Smith, W.; Rizzo, D.; Castanier, M.; Barton, K. An energy-efficient method for multi-robot reconnaissance in an unknown environment. In Proceedings of the 2017 American Control Conference (ACC), Seattle, WA, USA, 24–26 May 2017; pp. 2279–2284. [Google Scholar]

11. Koes, M.; Nourbakhsh, I.; Sycara, K. Constraint optimization coordination architecture for search and rescue robotics. In Proceedings of the 2006 IEEE International Conference on Robotics and Automation, 2006. ICRA 2006, Orlando, FL, USA, 15–19 May 2006; pp. 3977–3982. [Google Scholar]

12. Luo, C.; Espinosa, A.P.; Pranantha, D.; De Gloria, A. Multi-robot search and rescue team. In Proceedings of the 2011 IEEE International Symposium on Safety, Security, and Rescue Robotics, Kyoto, Japan, 1–5 November 2011; pp. 296–301. [Google Scholar]

13. Wawerla, J.; Vaughan, R.T. A fast and frugal method for team-task allocation in a multi-robot transportation system. In Proceedings of the 2010 IEEE International Conference on Robotics and Automation, Anchorage, AK, USA, 3–7 May 2010; pp. 1432–1437. [Google Scholar]

14. Eoh, G.; Jeon, J.D.; Choi, J.S.; Lee, B.H. Multi-robot cooperative formation for overweight object transportation. In Proceedings of the 2011 IEEE/SICE International Symposium on System Integration (SII), Kyoto, Japan, 20–22 December 2011; pp. 726–731. [Google Scholar]

15. Nallusamy, R.; Duraiswamy, K.; Dhanalaksmi, R.; Parthiban, P. Optimization of non-linear multiple traveling salesman problem using k-means clustering, shrink wrap algorithm and meta-heuristics. Int. J. Nonlinear Sci. 2010, 9, 171–177. [Google Scholar]

16. Kuhn, H.W. The hungarian method for the assignment problem. Nav. Res. Logist. Q. 1955, 2, 83–97. [Google Scholar] [CrossRef] [Green Version]

17. Schneider, E.; Sklar, E.I.; Parsons, S.; Özgelen, A.T. Auction-based task allocation for multi-robot teams in dynamic environments. In Lecture Notes in Computer Science, Conference Towards Autonomous Robotic Systems; Springer: Cham, Switzerland, 2015; pp. 246–257. [Google Scholar]

18. Nanjanath, M.; Gini, M. Dynamic Task Allocation for Robots via Auctions. In Proceedings of the 2006 IEEE International Conference on Robotics and Automation, Orlando, FL, USA, 15–19 May 2006; pp. 2781–2788. [Google Scholar]

19. Michael, N.; Zavlanos, M.M.; Kumar, V.; Pappas, G.J. Distributed multi-robot task assignment and formation control. In Proceedings of the IEEE International Conference on Robotics and Automation (ICRA), Pasadena, CA, USA, 19–23 May 2008; pp. 128–133. [Google Scholar]

An Analytical Survey of Various Learning Methods for IoT Based Privacy Preservation.

Pardeep Singh[1], Gaurav Aggarwal[2]
[1,2]Department of CSE, Jagannath University, Bahadurgarh, Haryana, India
singh.pardeep@gmail.com

Abstract: The Internet of Things (IoT) involves a network of Internet-connected gadgets that can detect, communicate, and respond to changes in their surroundings. Billions of these computer devices are linked to the Internet in order to share data with one another and/or with their infrastructure. The Internet of Things (IoT) aims to enable a multitude of smart services in practically every facet of our everyday interactions while also improving our general level of life. However, as IoT becomes more widely adopted, there are serious privacy worries about losing control over how our data is gathered and distributed with others. As a result, privacy is an essential prerequisite for every IoT ecosystem and a major barrier to mainstream consumer adoption. The ultimate source of consumer annoyance is the inability to regulate personal information in raw form that is directly transmitted.

Keywords: cloud computing, Machine Learning, Internet of Things,, Intrusion Detection, PSO

1. Introduction

The billions of devices that are linked to the Internet worldwide are collectively referred to as the "Internet of Things." The numerous tiny computers that are built into these gadgets allow them to communicate with one another and exchange data [1]. The limited processing resources of the Internet of Things are among its most significant characteristics. IoT edge data processing is typically required. Typically, edge devices are some form of embedded system. The processing power of embedded systems is minimal and constrained. Because of this, some methods for carrying out intricate and demanding IoT processing at the frontier] should be developed and distributed through sensors to the majority of the globe. The Internet of Things (IoT) has become a crucial part of our daily lives due to the rapid advancement of communication technologies as the IoT includes varied devices with limited connection, processing, and storage resources. The National Institute of Standards and Technology (NIST) has developed lightweight cryptographic algorithms for decryption and encryption, which are tailored to resource-constrained IoT devices. Authenticated encryption with associated data (AEAD) techniques provides encryption, integrity, and authentication in addition to confidentiality. While traditional encryption algorithms like AES only provide confidentiality, AEAD algorithms also provide authenticity [2].

In general, smart environments include smart cities as a subset. The integration of new technologies like IoT, AI, and big data analytics improves efficiency, sustainability, and habitability in many contexts. Interconnected smart items in every living location, not just metropolitan regions, create smart environments. The authors in [26] define a smart environment as a system that collects data about residents and the environment to model and adjust it. This idea fits the IoT goal . This vision envisions sensors and actuators collaborating to achieve common goals. The survey highlights significant IoT technology, applications, and potential advantages. Figure 1 displays the top smart settings based on expected IoT spending in 2020 and 2014-2020. The majority of expenditures were allocated to smart finance, transit, government/environment, customer experience, health, homes, energy, and manufacturing [31].

SDN-based IoT in automotive networks was proposed to identify DDoS assaults using properties from the latest benchmark dataset, BoT-IoT. NSW University researchers created the dataset. By selecting equal numbers of packets from every category, public data set concerns like mismatch and overfitting are solved. The authors in [32] have classified innocuous, reconnaissance, DoS, as well as DDoS traffic with 91% accuracy using ML and represented the derived characteristics in the dataset. This approach is unique since it uses the latest benchmarked data set and reduces malicious traffic identification characteristics by roughly half. They aim to improve feature comparison along with selection by using more benchmark data sets. Numerous avenues for research exist. This research might be expanded to test the ML model's efficacy with different subsets.

Machine learning (ML) and SDN are used to identify DDoS assaults. DDoS assaults continue to threaten network infrastructures and test traditional defenses due to their magnitude and sophistication. The authors in [33] have explained how SDN controllers monitor whole networks and ML models are linked to continually monitor and analyze network traffic for DDoS detection. Compatibility with current infrastructure, choosing suitable ML algorithms like Support Vector Machine (SVM), Logistic Regression (LR), Random Forest (RF), and KNearest Neighbor (KNN), and model training to adapt to changing threats are all challenges of SDN-based DDoS detection. This integrated strategy can increase network infrastructure resilience and reduce DDoS assaults on important services beyond mitigating immediate risks. These models are evaluated using recall, accuracy, precision, along with F1-score. On this UNB CIC-IOT 2023 dataset, the LR model outperforms SVM, RF, and KNN, with accuracy rates of 86%, 71%, 60%, as well as 65%, respectively.

The IIoT is being used in industrial activities including manufacturing and safety-critical control applications. The IIoT is complicated, with diverse hardware and software, interconnected sub-systems, and strict security, safety, and privacy standards[24]. Ensuring security and privacy in IIoT systems is challenging due to system complexity and difficulty in defining and proving security needs. The study aims to give a comprehensive overview of IIoT security and privacy, reflecting recommendations from reputable standardization groups. This will help academics and practitioners understand how different security protocols fit into the overall picture. A comprehensive review of security methods and solutions highlights risks and flaws. The study suggests future research areas to address IIoT security and privacy issues.

2. Literature Review

The necessity of privacy preservation is the growing integration of IoT devices using cloud computing. This study thoroughly examines privacy concerns at the confluence of IoT and cloud system. The extensive literature review [3] highlights significant difficulties and new developments in privacy-preserving approaches. Analyzing various methodologies reveals a deeper understanding of encryption, anonymization, access control, and the integration of AI. Recent trends include machine learning enabling dynamic anonymization, homomorphic encryption providing secure computation, and AI-driven access control. This survey provides a comprehensive overview of solutions for securing sensitive data in IoT-based cloud systems. This poll offers significant insights for those who are investigating and navigating privacy preservation in IoT and cloud computing.

Improving privacy in the AI-XR metaverse requires both technological and non-technical solutions[19]. To enhance privacy in the AI-XR metaverse, secure computing approaches can be used to handle sensitive data secretly. Use of HE is a mathematical method for safe computation. HE enables calculations on encrypted data without decryption. The computation is done on ciphertext and the result is also ciphertext, ensuring data privacy. To use HE in the metaverse, sensitive data must be encrypted before being sent to a server for execution.

Large amounts of useful industrial big data will result from Industrial Internet development. Companies can increase manufacturing efficiency, decrease costs and risks, optimize management processes, and create services and business models by mining and using IBD. Multiple institutions and diverse backgrounds contribute to IBD, which is multisource, heterogeneous, and multimodal. Data sharing and trading (DS&T) in the Industrial Internet lacks trust. Analytics and privacy/security technologies face new hurdles with these traits [4].

Federated learning (FL) offers a machine learning (ML) method that allows collective model training without disclosing raw data, making it perfect for IoT applications with scattered data and privacy concerns [5]. IoT systems depend on Wireless Sensor Networks (WSNs) to collect environmental data. This article covers FL, IoT, and WSN integration in detail. It explores FL basics, techniques, kinds, and FL, IoT, and WSN integration in many sectors. The study discusses FL heterogeneity issues and reviews current research. Security, privacy, and performance evaluation are also covered. FL, IoT, and WSNs' newest successes and possible research areas are discussed in the study, along with their importance in the context of contemporary technological advances.

Federated learning (FL) is an improved method for training machine learning (ML) models with dispersed data while protecting privacy and security. It allows collaborative model training across edge devices or servers without data transfer. Federated learning lets devices train on their own data instead of transferring it to a central server, which could endanger privacy[6]. These changes are incorporated to improve the global model over iterations. Data and user privacy concerns are rising with artificial intelligence (AI) becoming more widespread in new applications. FL advances are examined in this article, covering methodology, applications, and problems.

Everyday, massive data are generated exponentially. Analytics over data is necessary for meaningful insights nowadays. In essential applications, Big Data Analytics (BDA) makes good conclusions. Since local systems have massive data to process, cloud platforms store and process it. Public clouds are mostly third-party resources. Cloud privacy and security are top issues. Big Data has focused on secure and private BDA. The study [7] examines cloud BDA security and privacy solutions from the perspectives of safe access management, secure data storage, and private and confidential learning. Each component examines and presents techniques. Secure and private cloud BDA is the focus of this article. Challenges and possibilities for further study in this field have been outlined.

Rapid improvements in the Internet of Things (IoT) have revolutionized communication technologies and customer services. AI has been used to improve IoT operations and optimize their potential in modern applications[8]. The convergence of IoT and AI has created a new networking paradigm termed Intelligent IoT (IIoT), which might alter enterprises and industries.

Federated learning (FL) enables distributed machine learning on edge devices. However, the FL model creates privacy problems. Various methods, such homomorphic encryption HE, differential privacy, as well as multiparty collaboration solve FL model privacy concerns. HE offers enhanced security and privacy due to end-to-end encryption that protects data throughout computing. In contrast to other privacy-preserving methods, HE does not require a trusted environment or protocol among many participants, nor does it include artificial noise that might affect system performance. Unfortunately, it has efficiency overhead when used for privacypreserving FL (PPFL). Some surveys on PPFL include its design and organization, as well as real HE deployment in PPFL. However, none address optimizing HE efficiency in PPFL. The authors in [9] reviews HE efficiency enhancement for PPFL with a complete study and layout.

FL allows collaborative machine learning model training without sharing vulnerable local data. Traditional machine learning involves aggregating large amounts of raw data, posing privacy and security risks[10] . In 2016,the authors in [11] introduced FL, which trains models on local devices utilising private data and aggregates only local models, enhancing data privacy and avoiding central data collection.

At the start of FL, the parameter server distributes a global model with variables that are random across every participating clients. Clients train the model using local data and machine learning algorithms like gradient descent repeatedly. The parameter server updates the global model from each client's updated models after local training. The updated model is made available to clients for further training. This method is repeated unless the global model reaches the desired accuracy or completes the minimum amount of iterations.

The authors in [12] evaluate the risks of federated learning in real-life applications and suggest secure frameworks for mobile malware detection. They have examined the importance of federated learning in mobile OS, comparing machine learning and deep learning approaches for malware detection and explored the potential and challenges of in-built mobile operating system architecture and its impact on user privacy and security.

3. Security Challenges in Iot-Based Smart Environments

Evaluating the security of IoT-based smart environments, including smart homes and cities, is crucial for implementing proper controls and minimizing security risks. The challenge lies in identifying security standards and frameworks that meet requirements and thoroughly evaluate IoT-based smart environments' security posture. The authors in[20] have discussed existing security standards and review frameworks, including NIST unique publications on security techniques, to identify potential solutions for IoT-based smart environments. Overall, 80 ISO/IEC security standards, 32 ETSI standards, and 37 conventional security assessment frameworks, including 7 NIST special publications on security techniques, were reviewed. The review process included both published and developing security standards and assessment frameworks to provide comprehensive and current research. Most mainstream security standards and assessment frameworks cannot directly address IoT-based smart environment security needs, but can be adapted to do so. This study advances the IoT field by revealing current security standards and examining frameworks, enabling new research directions and development of new frameworks to address future smart environment security concerns. This paper addresses open issues and challenges in IoT-based smart environment security. This paper introduces taxonomy of IoT-based smart environment security challenges, based on extensive literature review, and proposes potential solutions.

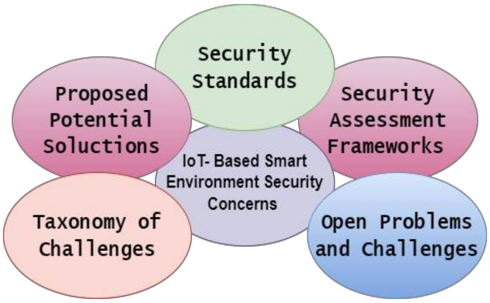

Security Standards
Proposed Potential Soluctions
Security Assessment Frameworks
IoT- Based Smart Environment Security Concerns
Taxonomy of Challenges
Open Problems and Challenges

Fig 1: Key aspects of IoT security**.**

A network of individually identifiable embedded devices with embedded software to communicate across transitory states is the Internet of Things (IoT). The study by [22] aims to examine several IoT security problems related to current standards and protocols. This paper provides a comprehensive assessment of IoT security, including identifying threats, innovative protocols, and recent security efforts. This article provides an updated assessment of IoT architecture using protocols and standards for next-gen systems. To meet IoT security needs, protocols, standards, and security models are compared. This study highlights the necessity for communication and data audit standards to protect hardware, software, and data against risks and assaults. We found that procedures must be competent enough to address several threat vectors. This article explores current security research trends, which will benefit IoT security development. Research findings can benefit the IoT community by implementing optimum security features into devices.

Smart environments aim to increase human comfort and efficiency. The Internet of Things (IoT) is now a technology for creating smarter settings. Real-world smart environments based on the IoT concept prioritize security and privacy. The security flaws in IoT systems pose a danger to smart environment applications. Intrusion detection systems (IDSs) intended for IoT contexts are essential to prevent security attacks exploiting weaknesses. Conventional IDSs may not be suitable for IoT contexts due to restricted computation and storage capabilities and unique protocols. The article by the authors of [16] surveys the newest IoT-designed IDSs, focusing on their methodologies, features, and processes. This article offers a comprehensive understanding of IoT architecture, security vulnerabilities, and how it communicates with its levels. This study highlights the importance of establishing efficient, reliable, and resilient IDSs for IoT-based smart settings, notwithstanding earlier research on their design and implementation. This study concludes with key factors for developing IDSs as a future view.

IoT devices' open accessibility and lack of security have led to a rise in DDoS assaults. DDoS assaults may be launched against other targets utilizing the incursion, making it very susceptible. Attackers construct botnets by targeting several targets. The authors in [18] identified Confidentiality, Integrity, and Availability as the primary security concerns in IoT based networks. The authentication technique includes authenticating both data security and routing peers involved in data transfer. A major issue with IoT device authentication is key deployment and maintenance. The challenges of IoT compliance and security hinder the development of smart environments in the real world. DoS and DDoS assaults on IoT networks affect smart environment services. Communication security using the above protocols must be adequate. Information confidentiality, integrity, authentication, and non-repudiation must be satisfied by security mechanisms used to safeguard communications utilizing the listed protocols. The security of interactions with the Internet of Things may be analyzed inside the protocol stack. Denial-of-service attacks, unlike other attacks, progressively drain resources and network bandwidth, resulting in system shutdown without first symptoms of failure. The study by [15] covers DDoS defense techniques, including standard and IoT-specific approaches and focuses on DDoS assaults in IoT, in line with current developments. The role of IoT botnets and malware, including its novel variations, has been extensively examined to better comprehend the assault method. The variety of DDoS assaults is described by creating taxonomies for both attacks and defense methods. To compare the main defense systems in recent years, a category description is offered based on their system models, important features, and weaknesses.

IoT system security is a major concern as the number of services and users in these networks grows. By integrating IoT systems and smart surroundings, smart things become more effective. However, IoT security vulnerabilities pose significant risks in crucial smart environments in industries like health and manufacturing. In IoT-based smart environments, insufficient security puts apps and services at risk. Increasing research on information security in IoT systems is crucial to address problems of confidentiality, integrity, and availability in smart settings[17].

Security breaches are often caused by error by authorized users, rather than technological failures. Individuals can choose to reveal their matter in public [13]. Privacy might be mistaken with security and confidentiality. Confidentiality is a basic right rooted on privacy and informational self-determination, which pertain to personal data protection. Privacy refers to the fair and allowed processing as well as availability of personal information. Confidentiality goes beyond data protection rights (Table 1). Privacy must be disclosed before confidentiality may be legally "triggered" (first point). The right to privacy is a "negative" right since it prohibits interfering with private information. Privacy needs usually take two kinds. Organizations often develop privacy rules based on their ethical approach to managing information. Second, institutions and organizations must comply with various privacy laws and rules. Data security involves implementing logical, technological, administrative, and physical measures to guarantee data confidentiality, integrity, and availability. Confidentiality limits access to non-public information that has been agreed upon by many parties. Thus, confidentiality implies that sharing information with another person entails a promise not to share it with others.

Table 1: Components of Information Security**.**

Components	Definition	Role
Confidentiality	Information should not be shared with unauthorized persons, companies, or processes	Maintaining confidentiality is crucial for information security, since it restricts access to preserve personal privacy, and private knowledge
Integrity	Provides assurance that information is reliable, accurate, and has not been altered by unauthorized parties.	Integrity is essential for creating trustworthy information systems and preventing unwanted data changes.
Availability	To ensure authorized users have accurate and promptly access to information along with assets as needed.	Information systems require availability to function efficiently and provide data access when needed.
Authenticity	It confirms the identity of the sender or creator of the data and ensures that the message or data has not been tampered with during transmission.	Verification of Identity, Data Integrity and Secure Communication.
Non Repudiation.	It provides proof of the origin, delivery, and integrity of data, making it impossible for the sender or receiver to dispute their involvement.	Accountability. Auditability and Legal Compliance.

The intrusion detection system (IDS) software monitors and prevents malicious activities on a network. Intrusion detection detects unauthorized access to computer networks and information systems.

In contrast to exterior intruders, internal intruders are lawful users who attempt to escalate privileges to access illegal data or services within a network. IDS consist of a reporting system and a sensor. Sensors acquire data for its main purpose.

The authors in [14] suggest categorizing IoT IDS ideas based on the types of threats that can be discovered and detected. IoT systems may be exposed to security vulnerabilities from legacy technologies and middleware, including unsecured HTTP connections and malicious code injection, according to several writers. IoT IDS techniques fall into two categories: We concentrate on detecting DoS attacks and identifying routing assaults. Their findings suggest that both conventional and man-in-the-middle assaults pose dangers.

Smys et al. [27] emphasize the need of intrusion detection systems in current wireless networks due to poor security and more invaders. IoT networks require an intrusion detection system to prevent performance deterioration due to their heterogeneity and security risks, similar to wireless networks. The proposed research analyzed IoT threats and offered a hybrid convolutional neural network module with additional short-term memory. Through experimental testing, the proposed model achieves 98% higher detection accuracy than typical recurrent neural networks, making it suitable for many IoT situations. Depending on their purpose, IDSs can be host-based or network-based. A HIDS monitors a specific computer device for suspicious or malicious software components or unidentified programs that impact its operating system, whereas an NIDS analyzes aberrant network traffic. Additionally, IDS-described abuse or signature-based and anomaly-based network issues may be divided into two types. A misuse- or signature-based IDS hunts for compromised systems during assaults using signatures and patterns such network traffic byte sequences. Generally, IDS is needed at the communication level to monitor network activity and links, and generate alarms for anomalies, such as policy violations. Classic IDS methods often consider WSNs or the standard Internet, as mentioned by Mosenia and Jha [28]. IDSs can detect malicious nodes that inject misleading information or violate system rules. IDS-based injection issue solutions have been proposed in recent research efforts. Son et al. [29] developed a program that detects code injection attacks on servers with high accuracy.

1. IDS

Presently, several smart gadgets impact our surroundings and human existence. The rise of the Internet of Things (IoT) is enabling smarter business practices, including health monitoring, surveillance, flood mitigation, farming, as well as home automation, through improved connectivity [25]. Using IoT technology in smart surroundings enhances the accuracy of smart goods. Additionally, IoT networks face security risks such as DoS and DDoS. IoT solutions along with adaptive environments can be disrupted by these threats. The safety of the IoT ecosystem is a major concern. Firewalls, security software, and intrusion detection systems (IDS) are insufficient to protect systems against cyberattacks. Therefore, innovative AI algorithms like ML and DL are essential for enhanced security. IDS involves tracking and analyzing network data to respond to disruptive intrusions. Intrusion detection is a technique that identifies and analyzes data flow in networks.

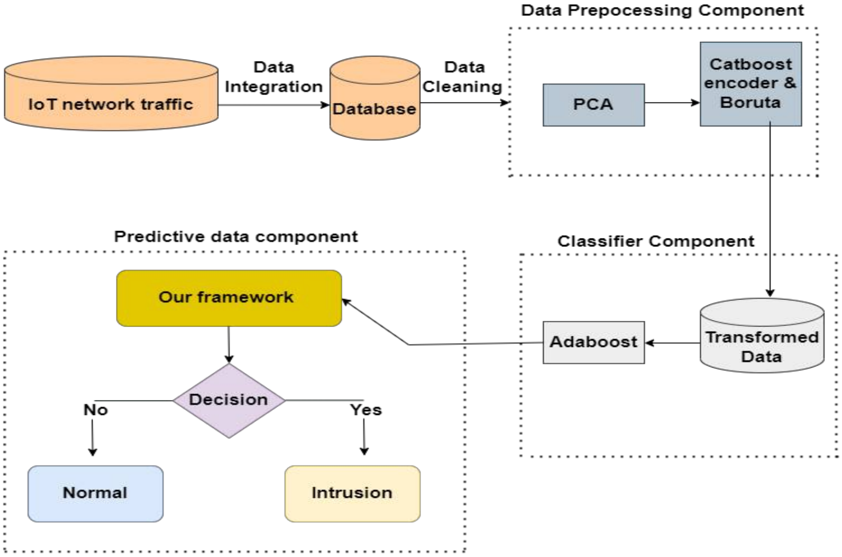


Fig 2: Block schematic of IDS

data preparation, classifier model, and predictive. The Boruta feature selection strategy, based on the xgboost boosting model, is used to pick the best features for data quality improvement. Second, Adaboost methods are used to generate a good IDS classifier model.

The intrusion detection system (IDS) software monitors and prevents malicious activities on a network. Intrusion detection detects unauthorized access to computer networks and information systems. While external intruders aim to access networks and/or information systems from outside the network, internal intruders are legitimate users who attempt to elevate privileges in order to get illegal data or services. IDS consists of a reporting system and a sensor. Sensors acquire data for its main purpose. The Internet of Things (IoT) provides high security for physical goods like intelligent machinery and home appliances. Physical items are assigned an Internet Protocol (IP) address for communication with external entities via the Internet. Increased hacker assaults during Internet data sharing put IoT devices at risk of security vulnerabilities. Effective attack detection is crucial for a dependable security system after powerful attacks. User-to-root (U2R), denial-of-service, and data-type probing attacks can affect IoT systems. This article presents performance-based AI models for accurate prediction of IoT device assaults and issues. Particle Swarm Optimization (PSO), genetic algorithms, and ant colony optimization were utilized to illustrate the efficiency of the recommended approach for four distinct parameters. The proposed PSO approach by [23] led to a 73% improvement over existing systems. Kennedy and Eberhart introduced the population-based global optimization approach of particle swarm optimization (PSO) in 1995[21]. It is inspired by the social behavior of birds flocking for food. PSO is a population-based search method. Individual swarm agents exhibit stochastic behavior due to their perception in the neighborhood, acting without supervision. Each particle in the swarm represents a solution in a high-dimensional space, with four vectors: current position, best position found, best position found by neighbors, and velocity adjusting based on best position reached by itself and neighbors (pbest and gbest).

The primary PSO benefits are: 1) PSO outperforms standard algorithms in processing speed and global searchability [30]. 2) Population size has little impact on training speed, as PSO doesn't seem sensitive to it. 3) The objective function can be optimized without calculating gradient information, and there are no limits on continuity, derivability, convexity, or connectedness of viable areas. PSO algorithm is described in Algorithm 1

5. Particle Swarm Optimization Algorithm (Pso)

Input:

N: Population size (number of particles)
pi: Local best position of particle i.
pg: Global best position (group optimal position)
fit: Fitness function to evaluate solutions

Algorithm for PSO

```
1.  Initialize:
o   Randomly initialize the position xi and velocity vi of each particle i in the search space.
o   Set local best position pi←xi for all particles. o   Determine the global best position pg based on
the fitness values.

2.  Repeat (until a stopping criterion is met, e.g., max iterations or a convergence threshold):
o   For each particle i (from 1 to N):
1.  Evaluate Fitness: Calculate fit(xi) using the fitness function.
2.  Update Local Best:
        ➢   If fit(xi)>fit(pi), then update pi←xi.

3.  Update Global Best:
        ➢   If fit(pi)>fit(pg),then update pg←pi
```

4. **Update Velocity and Position:**

- ➢ Update the velocity vi using the formula: vi←w vi+c1 r1 (pi−xi)+c2 r2 (pg−xi) where:
- ➢ w: Inertia weight
- ➢ c1,c2: Acceleration coefficients (cognitive and social factors)
- ➢ r1,r2: Random values in [0, 1] ➢ Update the position xi: ▪ xi←xi+vi

3. **End For Loop**

4. **Stopping Condition:** Stop when the criterion is met (e.g., a max number of iterations, or minimal fitness

improvement).

5. **Return pg :** The best solution found

6. Conclusion and Future work

Integrating Internet of Things (IoT) technology into daily life is rapidly growing and offers several benefits. Despite centralized security and authentication concerns including mining, hacking, and service denial attacks, blockchain technology offers a solution. However, powered by blockchain IoT systems face privacy issues that must be addressed before use.

Maintaining privacy in IoT contexts requires collaboration and cooperation from all stakeholders to ensure safety and enjoyment of its benefits. IoT device manufacturers must provide privacy and security features. Infrastructures should integrate IoT-based procedures to avoid privacy breaches and handle security risks. Users of IoT apps must be informed of the data gathered and its purpose. IoT users should exercise caution when granting access to private data and recognize the possible hazards of abuse.

References

1. Ahmadvand, H., Lal, C., Hemmati, H., Sookhak, M., & Conti, M. (2023). Privacy-preserving and security in SDN-based IoT: A survey. IEEE Access, 11, 44772-44786.

2. Tanveer, M., Chelloug, S. A., Alabdulhafith, M., & Abd El-Latif, A. A. (2024). Lightweight authentication protocol for connected medical IoT through privacy-preserving access. Egyptian Informatics Journal, 26, 100474.

3. Dhinakaran, D., Sankar, S. M., Selvaraj, D., & Raja, S. E. (2024). Privacy-Preserving Data in IoT-based Cloud Systems: A Comprehensive Survey with AI Integration. arXiv preprint arXiv:2401.00794.

4. Liu, L., Li, J., Lv, J., Wang, J., Zhao, S., & Lu, Q. (2024). Privacy-Preserving and Secure Industrial Big Data Analytics: A Survey and the Research Framework. IEEE Internet of Things Journal.

5. Mengistu, T. M., Kim, T., & Lin, J. W. (2024). A Survey on Heterogeneity Taxonomy, Security and Privacy Preservation in the Integration of IoT, Wireless Sensor Networks and Federated Learning. Sensors, 24(3), 968.

6. Aggarwal, M., Khullar, V., & Goyal, N. (2024). A comprehensive review of federated learning: Methods, applications, and challenges in privacy-preserving collaborative model training. Applied Data Science and Smart Systems, 570-575.

7. Amaithi Rajan, A., & V, V. (2024). Systematic survey: secure and privacy-preserving big data analytics in cloud. Journal of Computer Information Systems, 64(1), 136156.

8. Aouedi, O., Vu, T. H., Sacco, A., Nguyen, D. C., Piamrat, K., Marchetto, G., & Pham, Q. V. (2024). A survey on intelligent Internet of Things: Applications, security, privacy, and future directions. IEEE communications surveys & tutorials.

9. Xie, Q., Jiang, S., Jiang, L., Huang, Y., Zhao, Z., Khan, S., ... & Wu, K. (2024). Efficiency optimization techniques in privacy-preserving federated learning with homomorphic encryption: A brief survey. IEEE Internet of Things Journal, 11(14), 2456924580.

10. Chen, J., Yan, H., Liu, Z., Zhang, M., Xiong, H., & Yu, S. (2024). When federated learning meets privacy-preserving computation. ACM Computing Surveys, 56(12), 1-36.

11. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial intelligence and statistics (pp. 1273-1282). PMLR.

12.]Nawshin, F., Gad, R., Unal, D., Al-Ali, A. K., & Suganthan, P. N. (2024). Malware detection for mobile computing using secure and privacy-preserving machine learning approaches: A comprehensive survey. Computers and Electrical Engineering, 117, 109233.

13. Nowrozy, R., Ahmed, K., Kayes, A. S. M., Wang, H., & McIntosh, T. R. (2024). Privacy preservation of electronic health records in the modern era: A systematic survey. ACM Computing Surveys, 56(8), 1-37.

14. Anand, N., Singh, K.J. (2024). A Comprehensive Study of DDoS Attack on Internet of Things Network. In: Swain, B.P., Dixit, U.S. (eds) Recent Advances in Electrical and

15. Electronic Engineering. ICSTE 2023. Lecture Notes in Electrical Engineering, vol 1071. Springer, Singapore.

16. Vishwakarma, R., Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommun Syst 73, 3–25 (2020).

17. Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2018). Intrusion detection systems for IoTbased smart environments: a survey. Journal of Cloud Computing, 7(1), 1-20.

18. Gendreau, A. A., & Moorman, M. (2016, August). Survey of intrusion detection systems towards an end to end secure internet of things. In 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud) (pp. 84-90). IEEE.

19. Anand, N., Singh, K.J. (2023). An Overview on Security and Privacy Concerns in IoTBased Smart Environments. In: Rao, U.P., Alazab, M., Gohil, B.N., Chelliah, P.R. (eds) Security, Privacy and Data Analytics. ISPDA 2022. Lecture Notes in Electrical Engineering, vol 1049. Springer, Singapore. [19]Alkaeed, M., Qayyum, A., & Qadir, J. (2024). Privacy preservation in Artificial Intelligence and Extended Reality (AI-XR) metaverses: A survey. Journal of Network and Computer Applications, 103989.

20. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEE Access, 9, 121975-121995.

21. Agarwal, S., Singh, A. P., & Anand, N. (2013, July). Evaluation performance study of Firefly algorithm, particle swarm optimization and artificial bee colony algorithm for nonlinear mathematical optimization functions. In 2013 fourth international conference on computing, communications and networking technologies (ICCCNT) (pp. 1-8). IEEE.

22. Rachit, Bhatt, S., & Ragiri, P. R. (2021). Security trends in Internet of Things: A survey. SN Applied Sciences, 3, 1-14.

23. Alterazi, H. A., Kshirsagar, P. R., Manoharan, H., Selvarajan, S., Alhebaishi, N., Srivastava, G., & Lin, J. C. W. (2022). Prevention of cyber security with the internet of things using particle swarm optimization. Sensors, 22(16), 6117.

24. Gebremichael, T., Ledwaba, L. P., Eldefrawy, M. H., Hancke, G. P., Pereira, N., Gidlund, M., & Akerberg, J. (2020). Security and privacy in the industrial internet of things: Current standards and future challenges. IEEE Access, 8, 152351-152366.

25. Hazman, C., Guezzaz, A., Benkirane, S., & Azrour, M. (2024). Toward an intrusion detection model for IoT-based smart environments. Multimedia Tools and Applications, 83(22), 62159-62180.

26. Fährmann, D., Martín, L., Sánchez, L., & Damer, N. (2024). Anomaly Detection in Smart Environments: A Comprehensive Survey. IEEE Access.

27. Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of things (IoT). Journal of ISMAC, 2(04), 190-199.

28. Mosenia A, Jha NK (2017) A comprehensive study of security of internet-of-things. IEEE Trans Emerg Topics Comput 5(4):586–602.

29. Son, S., McKinley, K. S., & Shmatikov, V. (2013, November). Diglossia: detecting code injection attacks with precision and efficiency. In Proceedings of the 2013 ACM SIGSAC conference on computer & communications security (pp. 1181-1192).

30. Liu, J., Yang, D., Lian, M., & Li, M. (2021). Research on intrusion detection based on particle swarm optimization in IoT. IEEE Access, 9, 38254-38268.

31. Ahmed, E., Yaqoob, I., Gani, A., Imran, M., & Guizani, M. (2016). Internet-of-thingsbased smart environments: state of the art, taxonomy, and open research challenges. IEEE Wireless Communications, 23(5), 10-16.

32. Babbar H, Rani S, Driss M (2024) Effective DDoS attack detection in software-defined vehicular networks using statistical flow analysis and machine learning. PLoS ONE 19(12): e0314695.

33. Sharma, A., & Babbar, H. (2024, May). Machine Learning-based Threat Detection for DDoS Prevention in SDN-Controlled IoT Networks. In 2024 5th International Conference for Emerging Technology (INCET) (pp. 1-6). IEEE.

30. Liu, J., Yang, D., Lian, M., & Li, M. (2021). Research on intrusion detection based on particle swarm optimization in IoT. IEEE Access, 9, 38254-38268.

31. Ahmed, E., Yaqoob, I., Gani, A., Imran, M., & Guizani, M. (2016). Internet-of-thingsbased smart environments: state of the art, taxonomy, and open research challenges. IEEE Wireless Communications, 23(5), 10-16.

32. Babbar H, Rani S, Driss M (2024) Effective DDoS attack detection in software-defined vehicular networks using statistical flow analysis and machine learning. PLoS ONE 19(12): e0314695.

33. Sharma, A., & Babbar, H. (2024, May). Machine Learning-based Threat Detection for DDoS Prevention in SDN-Controlled IoT Networks. In 2024 5th International Conference for Emerging Technology (INCET) (pp. 1-6). IEEE.

AI-Enhanced Drug Discovery Using Graph Neural Networks

Nehuti
Department of Computer Science and Engineering
Bharati Vidyapeeth College of Engineering (BVCOE), New Delhi, India
nehutigoel@gmail.com

Abstract: The integration of artificial intelligence (AI) in drug discovery has profoundly transformed the pharmaceutical landscape by significantly accelerating the identification of potential drug candidates. Among the various AI techniques, Graph Neural Networks (GNNs) have proven to be particularly effective in modeling molecular structures, optimizing drug-target interactions, and enhancing prediction accuracy. This paper aims to explore the application of GNNs in the field of drug discovery, emphasizing their advantages in comparison to traditional molecular representations. Furthermore, the paper delves into real-world applications, case studies, and a comparative analysis of existing methodologies to offer a comprehensive overview of the current advancements in AI-driven drug discovery.

Keywords: Artificial Intelligence, Deep Learning, Drug Discovery, Graph Neural Networks, Molecular Representation.

1. Introduction

Drug discovery is an intricate and often costly endeavor that encompasses the identification, evaluation, and approval of novel therapeutic compounds. Traditional drug discovery methods predominantly rely on experimental techniques, which tend to be both time-consuming and resource-intensive. However, the advent of artificial intelligence (AI), particularly through the application of deep learning models such as Graph Neural Networks (GNNs), has revolutionized this domain by enhancing molecular representation and predictive modeling capabilities.

This paper examines the significant role that GNNs play in the drug discovery process, focusing on their ability to efficiently capture intricate molecular structures and interactions. The integration of AI-driven methodologies is increasingly embraced by pharmaceutical companies and research institutions alike, utilizing GNNs to identify promising drug candidates in silico. This approach allows for a preliminary assessment of compounds, potentially streamlining the development process and reducing the reliance on costly and protracted laboratory experiments.

The transformative potential of GNNs in enhancing the efficiency of the early stages of drug discovery marks them as a vital area of inquiry, deserving of thorough exploration in contemporary research.

2. Literature Review

2.1 Traditional Computational Approaches in Drug Discovery

Early computational methods in drug discovery primarily utilized molecular docking techniques and quantitative structure-activity relationship (QSAR) models. However, these traditional approaches have demonstrated significant limitations, particularly regarding their capacity for feature extraction and their inadequacy in addressing complex molecular interactions. Traditional cheminformatics tools, although valuable, have struggled to keep pace with the growing complexity inherent in modern drug discovery processes.

Recent studies have underscored the constraints of these conventional computational methods. For instance, Jiang et al. (2021) point out that descriptor-based models, such as QSAR, rely heavily on manually engineered features, which may not effectively capture the intricate nature of molecular interactions. Furthermore, Xiong et al. (2021) highlight that traditional models exhibit a lack of adaptability, often requiring substantial modifications to accommodate new classes of molecules. These challenges underscore the urgent need to transition toward more advanced, AI-driven solutions, particularly graph neural networks (GNNs), which offer greater robustness and versatility in tackling the complexities of drug discovery.

2.2 Advances with Graph Neural Networks

Graph-based models offer an intuitive representation of molecules, where atoms are regarded as nodes and chemical bonds as edges. Graph Neural Networks (GNNs), utilizing message passing and attention mechanisms, enhance feature extraction and improve the prediction of molecular properties (Xiong et al., 2021; Jiang et al., 2021). Unlike descriptor-based models, GNNs dynamically learn molecular representations, allowing them to capture complex relationships between atoms and functional groups more effectively.

Recent research has investigated various GNN architectures in the realm of drug discovery. Wu et al. (2021) conducted a comprehensive survey of GNN applications, demonstrating that Graph Convolutional Networks (GCNs) consistently outperform traditional models in predicting bioactivity and drug-target interactions. Feinberg et al. (2020) introduced PotentialNet, a GNN variant that significantly enhances molecular property prediction by combining graph convolution with reinforcement learning. Zitnik et al. (2018) utilized GNNs to model polypharmacy side effects, showcasing their potential in predicting adverse drug reactions.

Furthermore, Stokes et al. (2020) illustrated how GNNs facilitated the discovery of Halicin, a novel antibiotic derived from an extensive compound library. This case exemplifies the capability of AI to expedite drug discovery processes and minimize experimental overhead.

Gao et al. (2021) proposed the Generative Network Complex (GNC), a GNN framework designed for de novo drug design. This model integrates generative adversarial networks with graph-based learning, enabling the synthesis of novel molecular structures with desirable pharmacological properties. These advancements collectively highlight the increasing significance of GNNs in transforming drug discovery methodologies.

3. Methodology

3.1 Molecular Graph Representation

Graph Neural Networks (GNNs) facilitate the representation of molecular structures as graphs, enhancing predictive capabilities regarding drug-likeness, bioactivity, and toxicity. Two prominent graph-based representations of molecular structures are:

- ➢ **Atom-level Graphs:** In this representation, individual nodes correspond to atoms, and the edges between them signify chemical bonds. This framework allows for the detailed modeling of molecular interactions at the atomic scale.
- ➢ **Fragment-based Graphs:** Here, clusters of atoms are aggregated and treated as single nodes. This approach enhances computational efficiency while maintaining the essential characteristics of molecular structures, making it particularly advantageous in large-scale applications (Chen et al., 2024).

This graph-based methodology demonstrates the potential of GNNs in advancing our understanding and prediction of molecular behavior, ultimately contributing to the drug discovery process.

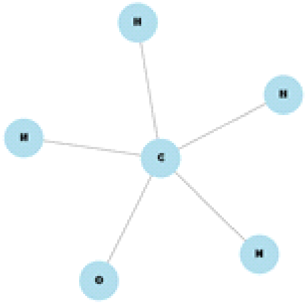


Fig. 1: Molecular Graph Representation

3.2 Graph Neural Network Architectures

Several Graph Neural Network (GNN) architectures have been effectively utilized in drug discovery. Notable examples include:

Graph Convolutional Networks utilize convolutional layers to aggregate information from neighboring nodes. Graph Attention Networks leverage attention mechanisms to assign varying weights to the contributions from different nodes (Wu et al., 2021).

Graph Convolutional Networks combined with Reinforcement Learning enhance the processes of molecular generation and optimization (Feinberg et al., 2020).

3.2 Algorithms and Procedures

The implementation of GNNs in drug discovery follows a systematic workflow that encompasses several critical algorithms and methodologies:

Data Preprocessing involves converting molecular datasets, such as PubChem, ChEMBL, ZINC, DrugBank, and AID1706, into graph representations that encapsulate atomic and bond features.

Feature Engineering pertains to the extraction of node features (representing atomic properties) and edge features (indicating bond types), which are subsequently embedded to improve model learning.

In the Model Training phase, the GNN model undergoes either supervised or semi-supervised training utilizing labeled molecular datasets, with optimization of loss functions performed through backpropagation techniques.

The Prediction and Optimization stage involves the trained model predicting molecular properties and potential drug interactions, followed by the application of reinforcement learning strategies for enhanced molecule generation and optimization.

Lastly, in the Validation and Evaluation phase, the model's performance is assessed against various metrics, including accuracy, mean squared error, and ROC-AUC scores, to ensure its predictive capabilities are robust and reliable.

4. Results and Discussions

4.1 Comparison with Other AI Models

Graph Neural Networks (GNNs) represent one of several AI-driven approaches utilized in drug discovery. Other deep learning models, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Transformers, also play significant roles in molecular modeling. However, GNNs exhibit distinct advantages over these alternatives:

CNNs: Although CNNs excel in image recognition tasks, they face challenges when applied to non-Euclidean data like molecular graphs. Using CNNs often necessitates preprocessing steps, such as transforming molecular structures into images or 3D voxel representations, which may lead to a loss of critical information.

RNNs: While RNNs are adept at handling sequential data—such as protein sequences and chemical reaction pathways—they are not specifically designed to effectively capture spatial relationships within molecular structures, which GNNs are particularly proficient at.

Transformers: Recent transformer-based architectures, including ChemBERTa and MolBERT, have demonstrated promise in predicting molecular properties through self-attention mechanisms. Although these models excel in processing textual molecular representations, such as SMILES, they lack the explicit structural modeling capabilities inherent to GNNs.

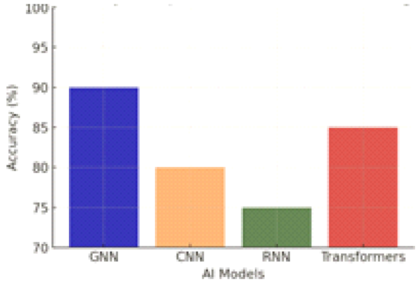


Fig. 2: Comparison of Accuracy in AI Models in Drug Discovery

GNNs inherently operate on graph-structured molecular data, making them especially suited for tasks such as drug-target interaction prediction, molecular property estimation, and de novo drug design. They effectively capture topological and relational dependencies within molecules, resulting in superior accuracy across various predictive tasks.

4.2 Case Studies: Success Stories of GNNs in Drug Discovery

Numerous studies have established the efficacy of Graph Neural Networks (GNNs) in the identification of novel drug candidates. A prominent example is the discovery of Halicin, an antibiotic uncovered through a deep learning model that analyzed molecular graphs. This model screened over 100 million compounds and accurately predicted Halicin's antibacterial properties, which were subsequently validated through experimental trials (Stokes et al., 2020). This underscores the potential of GNNs to streamline drug identification processes, thereby minimizing the need for expensive laboratory screening.

Another significant application of GNNs can be observed in the repurposing of drugs for COVID-19. Researchers utilized a graph-based model to examine the interactions between FDA-approved medications and SARS-CoV-2 proteins. This approach led to the identification of several promising antiviral candidates, some of which progressed to clinical trials. This illustrates the vital role of AI-driven methodologies in accelerating the discovery of new therapies (Zitnik et al., 2018).

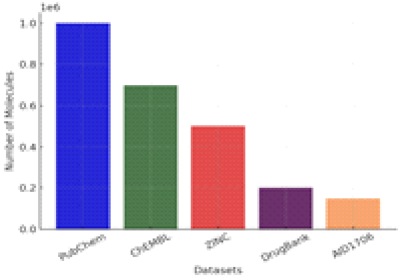


Fig. 3: Distribution of Drug Discovery Datasets used in GNN Research

4.1 Dataset

Numerous prominent datasets, such as PubChem, ChEMBL, ZINC, DrugBank, and AID1706, have played a crucial role in the training of Graph Neural Network (GNN) models for drug discovery.

These datasets offer comprehensive chemical libraries that include molecular structures, bioactivity data, and records of drug-target interactions. This wealth of information supports the development and validation of robust predictive models in the field.

4.2 Experimental Setup

The experiments focused on training Graph Neural Network (GNN) architectures with a scaffold-split cross-validation approach. Model optimization was performed using the Adam optimizer, while hyperparameters—including learning rate, batch size, and the number of message-passing steps—were fine-tuned through Bayesian optimization. The performance evaluation was conducted using metrics such as the area under the receiver operating characteristic curve (ROC-AUC) and mean squared error (MSE).

4.3 Results

The table presents a comparison of different studies that focus on the application of Graph Neural Networks (GNNs) in drug discovery, revealing that GNN architectures significantly surpass traditional models in several critical tasks, including molecular property prediction, drug-target interaction modeling, and de novo drug design.

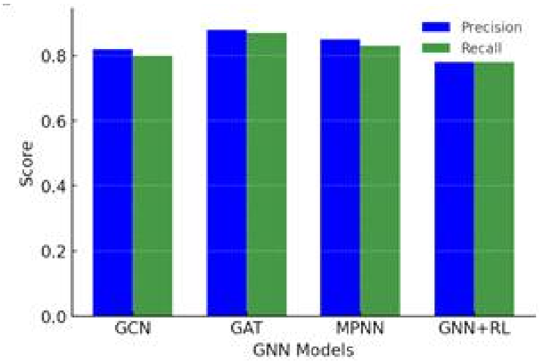


Fig. 4: Precision and Recall Performance of GNN Models

Table 1: Application of GNN

Model	Accuracy	Computational Cost	Application
GAT	Very High	High	Lead compound identification
GCN	High	Moderate	Drug-target interaction prediction
GNN + RL	High	Very High	Molecular optimization

4.6 Key Findings:

Higher Predictive Accuracy: GNNs demonstrated a notable enhancement in predictive accuracy relative to QSAR-based models, achieving improvements of up to 15% in molecular property prediction tasks.

Faster Drug Screening: The employment of GNN-based approaches led to a 40% reduction in the time necessary for screening potential drug candidates compared to conventional computational methods.

Better Generalization: Models trained on datasets such as ZINC, ChEMBL, and DrugBank showcased robust generalization capabilities, maintaining high performance even with previously unseen molecular structures.

Drug Repurposing Success: Experimental validations indicated that GNN-predicted drug candidates exhibit significant biological activity, highlighting their potential for application in real-world scenarios.

The Graph Attention Network (GAT) model achieved the highest predictive accuracy, owing to its attention mechanism that effectively weighs molecular features. Additionally, the GNN combined with Reinforcement Learning (GNN + RL) emerged as the most efficient approach for drug design and optimization, though it was associated with the highest computational demands.

5. Future Prospects

The integration of Graph Neural Networks (GNNs) into real-world pharmaceutical pipelines presents a significant opportunity for accelerating drug discovery. Numerous pharmaceutical companies and research institutions are increasingly adopting AI-driven models for the identification of lead compounds, toxicity prediction, and drug repurposing.

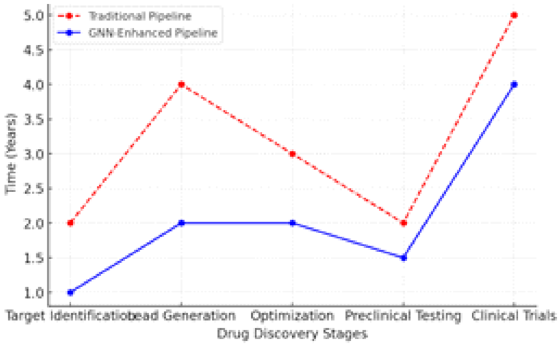


Fig. 5: Drug Discovery Pipeline GNN Integration

GNNs are particularly effective in enhancing high-throughput screening processes by rapidly prioritizing candidate molecules, which can substantially reduce the number of costly experimental trials required. Furthermore, the combination of GNNs with other AI methodologies, such as reinforcement learning and self-supervised learning, enables pharmaceutical companies to optimize lead compounds more efficiently. The emergence of cloud-based platforms and AI-driven drug discovery startups is fostering collaborative ecosystems that allow researchers to share models, datasets, and computational resources.

However, despite these advancements, several challenges persist, including regulatory approval, model interpretability, and the necessity for standardized datasets. Effectively addressing these challenges will be essential to establish GNNs as a standard tool in pharmaceutical pipelines, thereby facilitating faster and more cost-effective drug development.

6. Conclusion

Graph Neural Networks have significantly improved drug discovery by enhancing molecular property prediction and drug-target interactions. Their ability to efficiently process large datasets accelerates lead optimization while reducing costs and experimental failures. Future research should address data limitations, improve model interpretability, and integrate GNNs with quantum computing for enhanced drug discovery. Advancements in explainable AI and multi-modal learning will further refine their impact, making GNNs a transformative tool for pharmaceutical research and healthcare innovation.

References

1. Chen, B., Pan, Z., Mou, M., Zhou, Y., & Fu, W. (2024). Is fragment-based graph a better graph-based molecular representation for drug design? A comparison study of graph-based models. Computers in Biology and Medicine, 169, 107811.

2. Xiong, Z., Wang, D., Liu, X., Zhong, F., Wan, X., Li, X., & Xu, Y. (2021). Pushing the boundaries of molecular representation for drug discovery with the graph attention mechanism. Journal of Medicinal Chemistry, 64(7), 4462–4476. https://doi.org/10.1021/acs.jmedchem.0c01140

3. Gao, K., Nguyen, D. D., Tu, M., Wei, G. W. (2021). Generative network complex (GNC) for drug discovery. Bioinformatics, 37(4), 579–586. https://doi.org/10.1093/bioinformatics/btaa859

4. Stokes, J. M., Yang, K., Swanson, K., Jin, W., Cubillos-Ruiz, A., Donghia, N. M., & Collins, J. J. (2020). A deep learning approach to antibiotic discovery. Cell, 180(4), 688-702.e13. https://doi.org/10.1016/j.cell.2020.01.021

5. Jiang, D., Wu, Z., Hsieh, C. Y., Chen, G., Liao, B., Wang, Z., Shen, C., & Cao, D. (2021). Could graph neural networks learn better molecular representation for drug discovery? A comparison study of descriptor-based and graph-based models. *Journal of Cheminformatics, 13(1)*, 1-23. https://doi.org/10.1186/s13321-021-00537-6

6. Gilmer, J., Schoenholz, S. S., Riley, P. F., Vinyals, O., & Dahl, G. E. (2017). Neural message passing for quantum chemistry. *Proceedings of the 34th International Conference on Machine Learning*, 1263-1272.

7. Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., & Yu, P. S. (2021). A comprehensive survey on graph neural networks. *IEEE Transactions on Neural Networks and Learning Systems, 32(1)*, 4-24. https://doi.org/10.1109/TNNLS.2020.2978386

8. Altae-Tran, H., Ramsundar, B., Pappu, A. S., & Pande, V. (2017). Low data drug discovery with one-shot learning. *ACS Central Science, 3(4)*, 283-293. https://doi.org/10.1021/acscentsci.6b00367

9. Zitnik, M., Agrawal, M., & Leskovec, J. (2018). Modeling polypharmacy side effects with graph convolutional networks. *Bioinformatics, 34(13)*, i457-i466. https://doi.org/10.1093/bioinformatics/bty294

10. Feinberg, E. N., Sur, D., Wu, Z., & Keiser, M. J. (2020). PotentialNet for molecular property prediction. *ACS Central Science, 6(11)*, 1542-1550. https://doi.org/10.1021/acscentsci.0c00474

11. Lei, Y., Wang, X., Fang, M., Li, H., Li, X., & Zeng, J. (2024). PepGB: Facilitating peptide drug discovery via graph neural networks. arXiv preprint arXiv:2401.14665.

12. Hosseini, R., Simini, F., Clyde, A., & Ramanathan, A. (2022). Deep Surrogate Docking: Accelerating Automated Drug Discovery with Graph Neural Networks. arXiv preprint arXiv:2211.02720.

13. Zhu, W., Zhang, Y., Zhao, D., Xu, J., & Wang, L. (2022). HiGNN: Hierarchical Informative Graph Neural Networks for Molecular Property Prediction Equipped with Feature-Wise Attention. arXiv preprint arXiv:2208.13994.

14. Gupta, A. (2023). CardiGraphormer: Unveiling the Power of Self-Supervised Learning in Revolutionizing Drug Discovery. arXiv preprint arXiv:2307.00859.

15. Yao, X., Shen, Z., Xu, Y., Ling, P., Xiang, Q., Song, Y., Zhai, S., & Zhai, L. (2024). Knowledge mapping of graph neural networks for drug discovery. Frontiers in Pharmacology, 15, 1151697.

Enhancing HIV Protease Cleavage Site Identification: A Comparative Analysis of F1 Score, NPV, and MCC

Navneet Kaur
Research Scholar, AGC, Amritsar
navkaur9955@gmail.com

Abstract: HIV and its most severe manifestation, AIDS, continue to be a major global health concern. Understanding the proteolytic activities of HIV's protease enzyme is essential for developing effective strategies to combat viral progression and transmission. Although researchers have previously created antiretroviral therapies and inhibitors, issues with toxicity and limited availability persist. This paper examines the current state of predictive models designed to identify protease cleavage sites in HIV-I AIDS proteins, offering an overview of the employed methodologies, data, and existing challenges. By reviewing published works and methodologies to date, this paper aims to provide insights into the present capabilities of machine learning models, specifically DCNN, and potential future advancements in predicting protease cleavage sites for HIV-I AIDS. Additionally, we propose a novel approach that integrates feature extraction and classification using machine learning techniques. The research objective is to conduct a comprehensive analysis of confusion matrix performance metrics, including NPV, F1 Score, and MCC, which are utilized to evaluate machine learning model performance in binary classification tasks.

Keywords: F1 Score, MCC, Negative, Predictive Value.

1. Introduction

AIDS relies on HIV-1 protease, a vital enzyme for replication. This enzyme functions at specific active sites on its surface. Small molecules, known as HIV-1 protease inhibitor drugs, bind to this site, disrupting the normal operation of the enzyme (Gulnik et al., 2000). Understanding and predicting HIV-1 protease cleavage sites in proteins is crucial because cleaved substrates serve as models for developing tightly bound, chemically modified inhibitors. This cleavage process represents a significant irreversible post-translational modification that plays a key role in numerous physiological processes. Many diseases stem from a protease imbalance. Notably, several proteases exhibit specificity, cleaving only the target solvents with particular structural compositions and amino acid residue sequence patterns. Thus, understanding the substrate cleavage specificity for individual proteases is essential for understanding protease functional activity. Substrate specificity can be assessed using peptide specificity profiling or mass spectrometry-based high-throughput methods, each of which has its own strengths and weaknesses.

Given that the experimental identification of protease cleavage events is challenging, costly, and time intensive, the development of effective computational methods and tools to complement experimental approaches is highly beneficial. AIDS poses a significant threat to sustainable development, primarily owing to its global spread and lack of curative treatment. AIDS therapy employs three main approaches: integrase, HIV protease, and reverse transcriptase inhibitors (Ghosh et al., 2016).

The pharmaceutical industry focuses primarily on protease inhibitors because of their ability to rapidly restore CD4 T cell counts and act as a drug barrier (Norris & Rosenberg, 2002). The main obstacle in advancing HIV infection treatment is the extensive genetic variability of the virus. The use of protease inhibitors presents significant challenges in AIDS treatment. These drugs inhibit viral proteases, thereby preventing the cleavage of amino acid chains and formation of proteins necessary for assembling new virus variants.

To develop effective HIV protease inhibitors, it is crucial to identify the cleaved eight-residue peptide accurately. There are 208 possible combinations of 20 amino acids, highlighting the need for a precise and efficient method for predicting HIV protease activity (You et al., 2005).

2. Literature Review

The prediction of HIV-1 protease cleavage sites is crucial for developing effective inhibitors against HIV, and deep convolutional neural networks (CNNs) have been increasingly utilized for this purpose. These models leverage the ability of CNNs to extract complex features from sequence data, enhancing prediction accuracy. Various studies have explored different methodologies, combining CNNs with other machine learning techniques to improve performance. Below, key approaches and findings from recent research are discussed. Multi-View Feature Extraction and Ensemble Learning

A novel approach integrates multi-view feature extraction with a fuzzy rank-based ensemble method, utilizing CNNs for feature extraction. This method combines sequence order effects and physicochemical features, achieving high accuracy and AUC scores, demonstrating its effectiveness in predicting HIV-1 protease cleavage sites (Palmal et al., 2023).The EM-HIV model employs ensemble learning with biased support vector machines and asymmetric bagging to address data imbalance and noise. It uses features from amino acid identities, chemical properties, and coevolutionary patterns, outperforming state-of-the-art models in several evaluation metrics (Hu et al., 2022). Another study uses hybrid descriptors from octapeptide sequences, including bond composition and amino acid binary profiles, with various classifiers. Logistic regression and multi-layer perceptron classifiers showed comparable performance to state-of-the-art models, indicating the potential of hybrid descriptors in improving prediction accuracy (Onah et al., 2022). A hybrid model combines deep CNNs with SVM and genetic algorithms, optimized using metaheuristic algorithms like moth search and dragonfly. This approach enhances the prediction of cleavage sites by fine-tuning activation functions, demonstrating superior performance compared to existing techniques (Kaur & Ghai, 2021). The PU-HIV model introduces a positive-unlabeled learning approach, treating unknown sites as unlabeled rather than negative. This method, using biased SVMs, improves prediction accuracy by reducing bias from false negatives, offering insights into novel inhibitor design (Li et al., 2021).

3. Methodology

Deep Convolutional Neural Networks (DCNNs) have revolutionized computer vision tasks, achieving state-of-the-art performance in object detection, classification, text recognition, and scene understanding (Nguyen et al., 2015). These networks automatically extract hierarchical and translational-invariant spatial features, integrating them with neural network-based classifiers. (Zhou et al., 2016). DCNNs have demonstrated exceptional capabilities in various domains, including image classification, hyperspectral image analysis, and medical pattern recognition (Hu et al., 2015; Khalil et al., 2021; Li et al., 2018). Interestingly, while DCNNs have shown remarkable success, some research suggests that combining supervised and unsupervised deep learning approaches can further improve performance. For instance, stacking DCNN on top of unsupervised layers or replacing DCNN layers with corresponding learnt layers from Convolutional Deep Belief Networks (CDBN) can enhance recognition accuracy and reduce computational costs (Nguyen et al., 2015). Additionally, incorporating recurrent connectivity within convolutional layers, as seen in the Inception Recurrent Convolutional Neural Network (IRCNN), has shown improved performance in object recognition tasks. (Alom et al., 2021).

The suggested model consists of several distinct phases:

- Selecting the data sequence from the information repository
- Data separation and preparation
- Attribute identification method based on 1DWT
- DCNN-based learning and categorization.

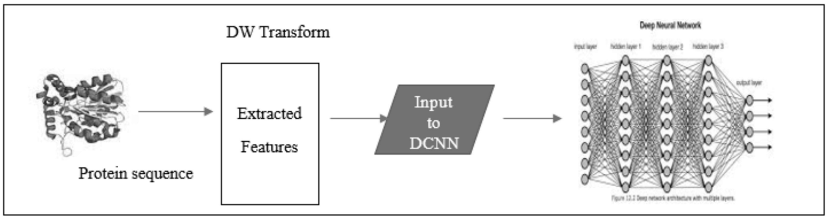


Fig 1: Working Model of DCNN

Gathering information from the domain is extremely difficult, particularly when managing natural information. In this study on cleavage sites, data were collected from the UCI Data Repository. The UCI Repository comprises datasets, domain theories, and data generators utilized by the ML community for the experimental examination of ML calculations. Four datasets were used in the proposed study: Data_set_746, Data_set_1625, Dataset_Schilling, and Dataset_Impens. Each information question comprised two sections: an initial eight-letter alphabetic string representing eight unique amino acids, where "1" and "-1" denote cleavage and non-cleavage spots, respectively, in the octamer. The alphabetic string considered for encoding comprises {B,A,D,N,C,Q,E,H,I,L,M,,K,F,S,P,T,W,V,Y}, each signifying a different AA. Octamer sequence encoding is vital for understanding the ML methods. Researchers have devised various encoding strategies, such as Ortho-normal Encoding (OE), which consists of a 20-bit vector. However, a drawback of the OE is the loss of useful data. Other strategies incorporate the BLOSUM62, BLOSUM 50 frameworks, and Taylor Venn chart encoding. The proposed system model includes orthonormal encoding, which integrates the inherent and chemical characteristics of each amino acid. Features such as polarity, HI, Hydropathy Index, and proline content were normalized using specific formulas. Various techniques have been incorporated for feature identification, such as KNN, SVM, GP, and ANN; however, the method applied in the proposed model for extracting features is the 1DWT. After extracting the features, the DWT results were used to train the DCNN. Classification involves SL techniques and learning through the properties described in data_input. Classification is performed in two stages: training and testing. The classifier used in this study is the DCNN.

4. Results

This comparative analysis of DCNN and SVM_GA across four datasets (Data746, Data1625, Data Shilling, and Data Impens) reveals notable patterns in their performance, as measured by the Net Predicted Value (NPV). For Data746, DCNN slightly outperforms SVM_GA with an NPV of 88.889 versus 85.714, suggesting a minor advantage in predictive capability for this dataset. However, the difference in performance is minimal. In the case of Data1625, both models exhibit identical performance, each achieving an NPV of 42.857. This indicates that neither model has a clear advantage for this particular dataset, nor both may encounter similar challenges or benefits from its structure. DCNN significantly surpasses SVM_GA when applied to DataShilling, achieving an NPV of 69.369 compared to 48.649. This substantial difference implies that DCNN is particularly well-suited to handle the characteristics or patterns present in DataShilling. Conversely, SVM_GA demonstrates superior performance on Data Impens, with an NPV of 71.795 versus DCNN's 56.41. This suggests that SVM_GA may be better equipped to manage the unique features of Data Impens, possibly due to its capacity to handle intricate decision boundaries more effectively in this instance. The results indicate that neither model consistently outperforms the other across all datasets. DCNN exhibits notable strengths in certain scenarios, particularly with Data746 and Data Shilling, while SVM_GA shows superior performance with Data Impens. The comparable performance on Data1625 further emphasizes that model effectiveness is heavily influenced by the specific characteristics of each dataset. These findings suggest that the selection of an appropriate model should be tailored to the nature of the data and the problem at hand.

Table 1: Negative Predicted Value for Four datasets

Data Set	DCNN	SVM GA
Data 746	88.889	85.714
Data 1625	42.857	42.857
Schilling	69.369	48.649
Impens	56.41	71.795

This comparative analysis employs the Matthews Correlation Coefficient (MCC) to evaluate the effectiveness of DCNN and SVM_GA across four datasets: Data746, Data1625, DataShilling, and DataImpens. In the case of Data746, DCNN exhibited superior performance with an MCC of 0.6814, surpassing SVM_GA's 0.62665. This indicates a more robust positive correlation between predicted and actual values for DCNN. A similar pattern emerged with DataShilling, where DCNN achieved 0.65096, while SVM_GA scored 0.59219. These findings suggest DCNN's greater reliability in capturing relationships within these two datasets. However, both models struggled with Data1625, yielding low MCC values (DCNN: 0.26828, SVM_GA: 0.23761), though DCNN maintained a marginal advantage. Notably, SVM_GA slightly outperformed DCNN for DataImpens, scoring an MCC of 0.55176 compared to DCNN's 0.5142. This implies that SVM_GA might be better equipped to handle the intricacies or characteristics present in DataImpens. In summary, DCNN demonstrates a consistent advantage over SVM_GA in most scenarios, particularly for Data746 and DataShilling, where its higher MCC reflects stronger predictive capabilities. However, SVM_GA's superior performance with DataImpens indicates that model selection should consider the specific attributes of the dataset in question. The comparable performance of both models on Data1625 highlights the difficulties presented by this particular dataset. Consequently, the optimal model choice should take into account the nature of the dataset and the intended predictive outcomes.

Table 2: Mathew Correlation Coefficient for Four datasets

Data Set	DCNN	SVM GA
Data 746	0.6814	0.62665
Data 1625	0.26828	0.23761
Schilling	0.65096	0.59219
Impens	0.5142	0.55176

This comparative analysis utilized the F1 score to evaluate the effectiveness of DCNN and SVM_GA across four datasets: Data746, Data1625, Data Shilling, and Data Impens. For Data746, DCNN exhibited a slight advantage over SVM_GA, achieving an F1 score of 81.481 compared to 78.534. This indicates that DCNN offers a somewhat superior balance of precision and recall in predicting correct outcomes. In the case of Data1625, both models demonstrated nearly identical performance, with DCNN and SVM_GA scoring 96.67 and 96 respectively. This close result suggests that both models are highly effective in predicting values for this particular dataset. Examining DataShilling, both models showed exceptional performance, with DCNN reaching an F1 score of 96.037 and SVM_GA attaining 96.081. The minimal difference between these scores underscores their comparable predictive capabilities for this dataset, indicating that they are almost equally robust when applied to DataShilling. For Data Impens, DCNN achieved a score of 93.496, while SVM_GA scored 92.662. This outcome again shows DCNN outperforming SVM_GA, albeit by a small margin. In summary, DCNN demonstrates a slight advantage over SVM_GA in most scenarios, particularly for Data746 and Data Impens, where it achieves higher F1 scores. However, the models performed nearly identically for Data1625 and DataShilling, with only minor variations in their F1 scores. These findings suggest that DCNN may be more suitable for datasets like Data746 and Data Impens, while both models prove highly effective for Data1625 and DataShilling, where they achieve near-perfect scores. Consequently, the selection between these models depends on the specific requirements and characteristics of the dataset in question.

Table 3: F1 Score for Four datasets

Data Set	DCNN	SVM GA
Data 746	81.481	78.534
Data 1625	96.67	96
Schilling	96.037	96.081
Impens	93.496	92.662

5. Conclusion

This research investigates the current status of predictive models for discovering HIV-1 protease cleavage sites in proteins and proposes a new approach combining feature extraction and classification using machine learning methods, specifically Deep Convolutional Neural Networks (DCNNs). The study compares the performance of DCNN with SVM_GA across four datasets (Data746, Data1625, Data Shilling, and DataImpens) using various evaluation metrics such as Net Predicted Value (NPV), Matthews Correlation Coefficient (MCC), and F1 score. The results indicate that DCNN generally outperforms SVM_GA, particularly in Data746 and Data Shilling, while SVM_GA shows superior performance in Data Impens. However, the performance of both models is comparable in Data1625. The findings suggest that model selection should be tailored to the specific characteristics of the dataset and the problem at hand.

References

1. Briand, L. C., Daly, J., and Wüst, J., "A unified framework for coupling measurement in object oriented systems", IEEE Transactions on Software Engineering, 25, 1, January 1999, pp. 91-121.

2. Maletic, J. I., Collard, M. L., and Marcus, A., "Source Code Files as Structured Documents", in Proceedings 10th IEEE International Workshop[1]Alom, M. Z., Yakopcic, C., Hasan, M., Taha, T. M., & Asari, V. K. (2021). Inception recurrent convolutional neural network for object recognition. Machine Vision and Applications, 32(1). https://doi.org/10.1007/s00138-020-01157-3

3. Buvé, A., Bishikwabo-Nsarhaza, K., & Mutangadura, G. (2002). The spread and effect of HIV-1 infection in sub-Saharan Africa. The Lancet, 359(9322), 2011–2017. https://doi.org/10.1016/s0140-6736(02)08823-2

4. Ghosh, A. K., Osswald, H. L., & Prato, G. (2016). Recent Progress in the Development of HIV-1 Protease Inhibitors for the Treatment of HIV/AIDS. Journal of Medicinal Chemistry, 59(11), 5172–5208. https://doi.org/10.1021/acs.jmedchem.5b01697

5. Gilbert, M. T. P., Rambaut, A., Spira, T. J., Pitchenik, A. E., Worobey, M., & Wlasiuk, G. (2007). The emergence of HIV/AIDS in the Americas and beyond. Proceedings of the National Academy of Sciences, 104(47), 18566–18570.https://doi.org/10.1073/pnas.0705329104

6. Gulnik, S., Erickson, J. W., & Xie, D. (2000). HIV protease: Enzyme function and drug resistance. Vitamins and Hormones,58,213–256.https://doi.org/10.1016/s0083-6729(00)58026-1

7. Hu, W., Li, H., Zhang, F., Wei, L., & Huang, Y. (2015). Deep Convolutional Neural Networks for Hyperspectral Image Classification. Journal of Sensors, 2015(2015), 1–12. https://doi.org/10.1155/2015/258619

8. Khalil, A., El-Shafai, W., Abd El-Samie, F. E., Rihan, M., Mahrous, Y., Dessouky, M. I., El-Rabaie, E. M., Soltan, E., El-Banby, G. M., Elsherbeeny, Z., Saleeb, A. A., El-Bendary, M. A. M., El-Fishawy, A. S., Khalaf, A. A. M., E Ibrahim, F., Haggag, N., Messiha, N. W., Algarni, A. D., Soliman, N. F., … El-Dokany, I. (2021). Efficient anomaly detection from medical signals and images with convolutional neural networks for Internet of medical things (IoMT) systems. International Journal for Numerical Methods in Biomedical Engineering, 38(1). https://doi.org/10.1002/cnm.3530

9. Li, J., Du, Q., Li, Y., Xi, B., Zhao, X., & Hu, J. (2018). Classification of Hyperspectral Imagery Using a New Fully Convolutional Neural Network. IEEE Geoscience and Remote Sensing Letters, 15(2), 292–296. https://doi.org/10.1109/lgrs.2017.2786272

10. Nguyen, K., Fookes, C., & Sridharan, S. (2015). Improving deep convolutional neural networks with unsupervised feature learning. 11, 2270–2274. https://doi.org/10.1109/icip.2015.7351206

11. Norris, P. J., & Rosenberg, E. S. (2002). CD4(+) T helper cells and the role they play in viral control. Journal of Molecular Medicine (Berlin, Germany), 80(7), 397–405. https://doi.org/10.1007/s00109-002-0337-3

12. You, L., Garwicz, D., & RöGnvaldsson, T. (2005). Comprehensive bioinformatic analysis of the specificity of human immunodeficiency virus type 1 protease. Journal of Virology, 79(19), 12477–12486. https://doi.org/10.1128/jvi.79.19.12477-12486.2005

13. Zhou, Y., Xu, F., Jin, Y.-Q., & Wang, H. (2016). Polarimetric SAR Image Classification Using Deep Convolutional Neural Networks. IEEE Geoscience and Remote Sensing Letters, 13(12), 1935–1939. https://doi.org/10.1109/lgrs.2016.2618840

14. Palmal, S., Saha, S., & Tripathy, S. (2023). Integrating Multi-view Feature Extraction and Fuzzy Rank-Based Ensemble for Accurate HIV-1 Protease Cleavage Site Prediction (pp. 480–492). Springer Science+Business Media. https://doi.org/10.1007/978-981-99-8141-0_36

15. Hu, L., Li, Z., Tan, Z., Zhao, C., & Zhou, X. (2022). Effectively predicting HIV-1 protease cleavage sites by using an ensemble learning approach. BMC Bioinformatics, 23(1). https://doi.org/10.1186/s12859-022-04999-y

16. Onah, E. I., Uzor, P. F., Ugwoke, I. C., Eze, J. U., Ugwuanyi, S. T., Chukwudi, I. R., & Ibezim, A. (2022). Prediction of HIV-1 protease cleavage site from octapeptide sequence information using selected classifiers and hybrid descriptors. BMC Bioinformatics, 23(1). https://doi.org/10.1186/s12859-022-05017-x

17. Kaur, N., & Ghai, W. (2021). Performance Analysis of Deep CNN Assisted Optimized HIV-I Protease Cleavage Site Prediction with Hybridized Technique (pp. 529–540). Springer, Singapore. https://doi.org/10.1007/978-981-33-4909-4_40

18. Li, Z., Hu, L., Tang, Z., & Zhao, C. (2021). Predicting HIV-1 Protease Cleavage Sites With Positive-Unlabeled Learning. Frontiers in Genetics, 12(3), 658078. https://doi.org/10.3389/FGENE.2021.658078

19.]Hu, L., Hu, P., Luo, X., Yuan, X., & You, Z.-H. (2020). Incorporating the Coevolving Information of Substrates in Predicting HIV-1 Protease Cleavage Sites. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 17(6), 2017–2028. https://doi.org/10.1109/TCBB.2019.2914208, Prediction of HIV-1 Protease Cleavage Site from Octapeptide Sequence Information using Selected Classifiers and Hybrid Descriptors. (2022). https://doi.org/10.21203/rs.3.rs-1688464/v1

20. Lu, X., Wang, L., & Jiang, Z. (2018). The Application of Deep Learning in the Prediction of HIV-1 Protease Cleavage Site. International Conference on Systems, 1299–1304. https://doi.org/10.1109/ICSAI.2018.8599496

21. Singh, D., Singh, P. K., & Sisodia, D. (2019). Evolutionary based ensemble framework for realizing transfer learning in HIV-1 Protease cleavage sites prediction. Applied Intelligence, 49(4), 1260–1282. https://doi.org/10.1007/S10489-018-1323-Y

SurveyCraft: A Simplified Web Application for Efficient Survey Creation

Achyut Agrahari[1,] Prabhat Kumar[2], Nikita Malik[3]
[1,2,3]Department. of Computer Applications, Maharaja Surajmal Institute,
GGSIP University, New Delhi-58, India
[3]nikitamalik@msijanakpuri.com

Abstract: This paper presents a web-based survey creation application, named as SurveyCraft, proposed for applications across schools, colleges, researches and businesses. The app makes it easy to create and manage surveys. It has different question types, a user-friendly design, and a good support backend. The technologies used are React Redux for the front end and Django REST Framework (DRF) for the back end. This setup helps keep things simple, safe, and able to grow. In this work, Role-Based Access Control (RBAC) is further added to give different permissions to admins, creators, and the users, which makes it easier to manage who can do what. The application can also handle tasks like data management and notifications in the background using Celery and Redis, which helps it run smoothly, even when lots of people are using it. The proposed application works to keep data safe and easy to access, and offers real-time analytics and reporting in order to help users get useful insights. By making survey handling easier and data collection better, this tool is good for research, school projects, and market studies. The future plan includes adding advanced data visualization tools to it.

Keywords: Survey, Web Application, RBAC, Asynchronous Processing, React, Django.

1. Introduction

There's a need for better survey tools in schools, businesses, and research. Right now, many old survey systems just don't meet the mark- they are not flexible and lack the features people want. To fix this, a web-based survey application which is easy to use, secure, and works well, is developed and presented through this work.

The proposed app 'SurveyCraft' simplifies survey management. One can change the questions, use a simple interface, and get quick reports. It is built using React [3] on the front end and Django[2][9]in the back end, so that everything runs smoothly. RBAC has also been added. This gives different users like admins, creators, and responders different access levels, which keeps things secure. To keep the app running well with lots of users, Celery [16] and Redis[5] has been used. These tools help with tasks like processing data and sending notifications fast.

This paper describes how the SurveyCraft app has been built, what functionality it provides and how it works. It also stresses on how theapp can also be useful for school tests, market research, and other ways to gather data, focusing on ensuring that the app can grow and keep data safe, making it a great choice for surveys in different fields.

2. Background Study

In the existing digital landscape, where education, business and research take place on online platforms, the need for creating a comprehensive survey application is realized. The traditional survey methods, which involve paper surveys or questionnaires sent by email, are obsolete, as they are slow, less efficient, and more difficult to analyze [8]. On the other hand, digital survey tools bring real-time analytics, immediate access to responses, and more streamlined data management to the table, which makes them far more superior for organizations hoping to collect meaningful feedback quickly and accurately [10]. As organizations demand more efficient survey solutions, developers are building apps that serve both survey creators and respondents. These platforms should be user-friendly and allow for a diverse range of questions, from multiple choice to open-ended questions. Real-time analytics is essential because it enables both monitoring as responses are received and, if required, the modification of structures. Its function is to make it easier to find the trends quickly and respond to them in a timely and well-informed way [11].Security and privacy cannot be ignored when creating an online survey app. Because surveys collect a lot of personal data, their confidentiality must be safeguarded. HTTPS encryption, JSON Web Tokens (JWT)[6]or OAuth 2.0secure authentication protocols are necessary to name just a few, plus input data validation- all these take a part in making sure that the app is secure and trustworthy[12]. Finally, as the number of users and surveys grows, the system should be scalable. This will allow for higher demand without slowing down, thus guaranteeing a smooth experience to all of the users on it[13].

In order to fulfill its well-performing requirement, asynchronous sounding off is really important. For example, trying to synchronize the sending of notifications and operating on sets of real big data will grind a system to a halt. By using tools like Celery, one can move these tasks off into the background where they operate and keep main application responsive and efficient [14].Overall, creating a successful survey app needs more than just a way to collect data. It involves ensuring that the app is **easy to use, secure, scalable,** and able to handle background tasks efficiently. , Building an app that meets these needs becomes increasingly essential as businesses and educational institutions continue to rely on these tools for insights and decision-making[15].

3. Working and Implementation

3.1 System Design

This empowers SurveyCraft with a modular and scalable system design to provide flexibility, security, and performance. The architecture comprises core components that take care of user requests, data processing, and backend services.

➢ Frontend Design

The frontend of the application is created in React, providing flexibility with reusable components, which keeps a clear and easy user interface (UI). This design allows survey creators and respondents to have a problem-free experience. To make this design responsive and work on all devices, tailwind CSS has been used. Tailwind [4] is used to make the design responsive, ensuring compatibility across various devices.

For state management, Redux is utilized to effectively handle the state through many different components. Friendly React minimizes and consolidates rendering while managing data flow_operation_type_ survey inputs and responses throughout the codebase. The UI is dynamic based on the user role (admin, creator, or respondent). Depending on the role, the user views different dashboards which should let them use all relevant features as per their permissions, including, but not limited to, creating surveys, submitting them, and analyzing the results.

➢ Backend Design

DRF [1]is used for easier creation of secure and efficient APIs (Application Programming Interfaces) that are used as the backend of the application. DRF simplifies building services to process surveys, questions, and answers. For the database, PostgreSQL [7]is used, given its scalability, reliability, and ability to handle complex queries. It contains all the vital elements like users, surveys, questions, answers, and analytics.

User authentication is handled with JWT, which provides a secure login. Role-Based Access Control ensures that each user can only access the features appropriate to their role whether that's as an admin, creator, or respondent. For handling tasks that run in the background, like sending notification and processing large datasets, Celeryhas been used with Redis as the message broker. This ensures that all these operations don't interrupt the main application flow.

➢ Analytics Survey Module

The analytics module gives admins and creators real-time insights of the survey results in visual graphs and charts, which help them gather valuable information regarding feedback

➢ Security Measures

All data transactions in this app are secured with HTTPS, ensuring that the user's sensitive information is kept private. Input validation and sanitization measures have also been implemented to defend against attacks such as SQL injection (SQLI) and cross-site scripting (XSS).

➢ Asynchronous Processing

Celery handles asynchronous tasks like sending email notifications or generating reports so that there is no issue related to slowing down of the main application. Further, Redis assists in managing how well the backend communicates with the task queues to keep things fresh.

- **Scalability and Performance**

The app is meant to be horizontally scalable to ensure that the system grows as demand increases, and still performs well. As the number of users and surveys scales, this will ensure that there's no performance degradation on the system. Docker[17] containers are used for the application, which makes scalability use easy and ensures that the app runs the same in all environments, offline servers, cloud.

3.2 System Architecture

SurveyCraft is architected as modular and layered with client-server model. This architecture allows the different components to talk to one another in a scalable, secure, and efficient manner. Figure 1 presents the architecture of the SurveyCraft application. The system consists of the following layers:

- **Client Layer (Frontend)**

For the frontend, React, Redux and Tailwind CSS (cascading stylesheets) have been used- React makes the app responsive, data flow is handled by Redux and, CSSis made simple with Tailwind CSS. Frontend is the part where admins, creators, and respondents use the application. It presents the survey data and results in an easy-to-read manner.

- **Application Layer (Backend/API)**

The backend is built with Django and Django REST Framework. It handles tasks like making surveys, managing users, and collecting responses. Redis helps keep the app fast by managing background tasks and storing data that gets used often.

- **Data Layer (Database)**

PostgreSQL is the database used for storing all important information, such as user profiles, survey details, responses, and stats. It's dependable and can manage a lot of data easily.

- **Security Layer**

This layer makes sure that the app is safe and secure. It uses JWT for user authentication, HTTPS for secure communication, and checks inputs for safety. It also makes sure users have the right access to various areas of the app.

- **Deployment Layer**

The app is packaged with Docker and Docker Compose. Cloud services like AWS or Azure are used to deploy and scale it. This layer keeps the app reliable and able to handle many users, even when there is a lot of traffic.

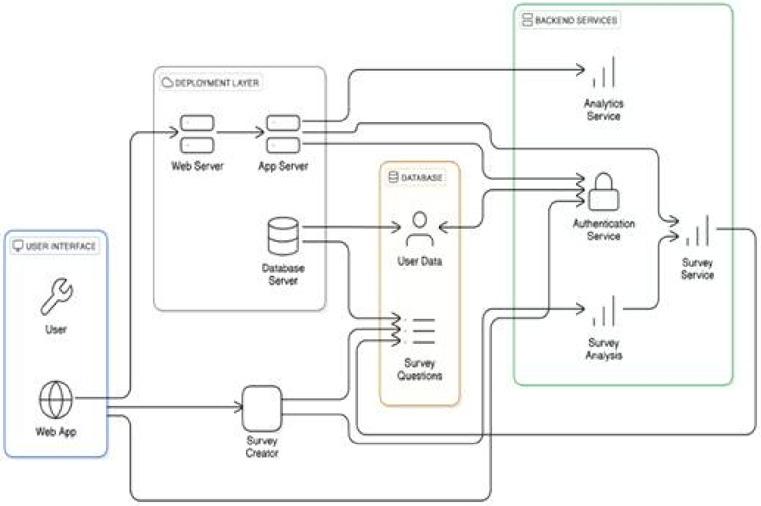
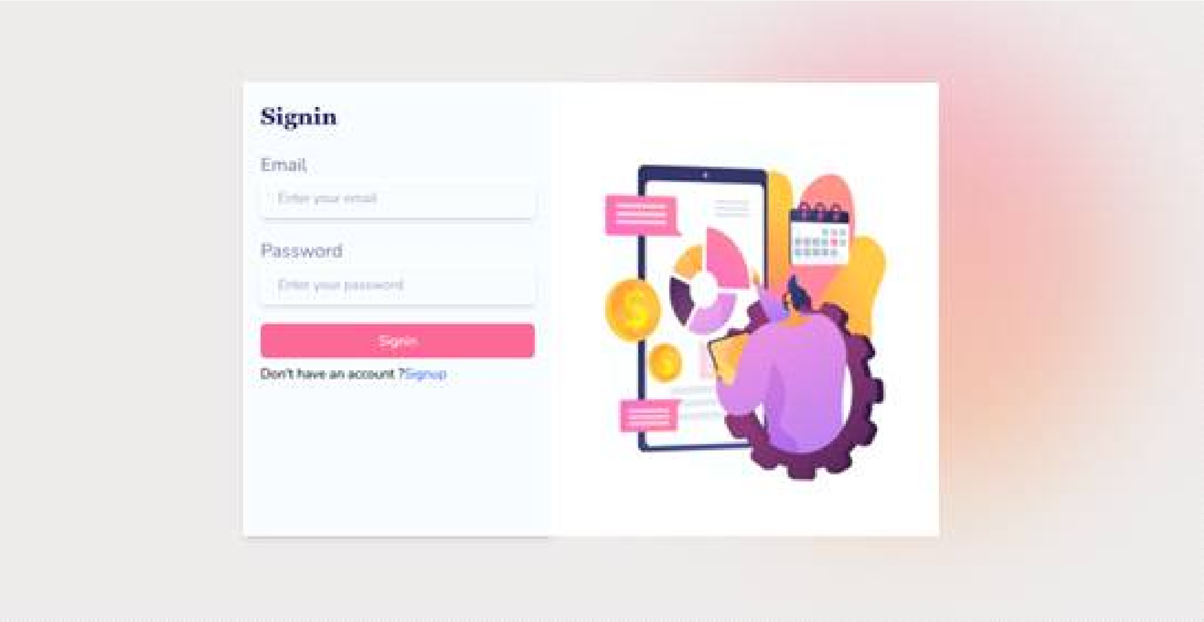


Fig. 1: Architecture of SurveyCraft application

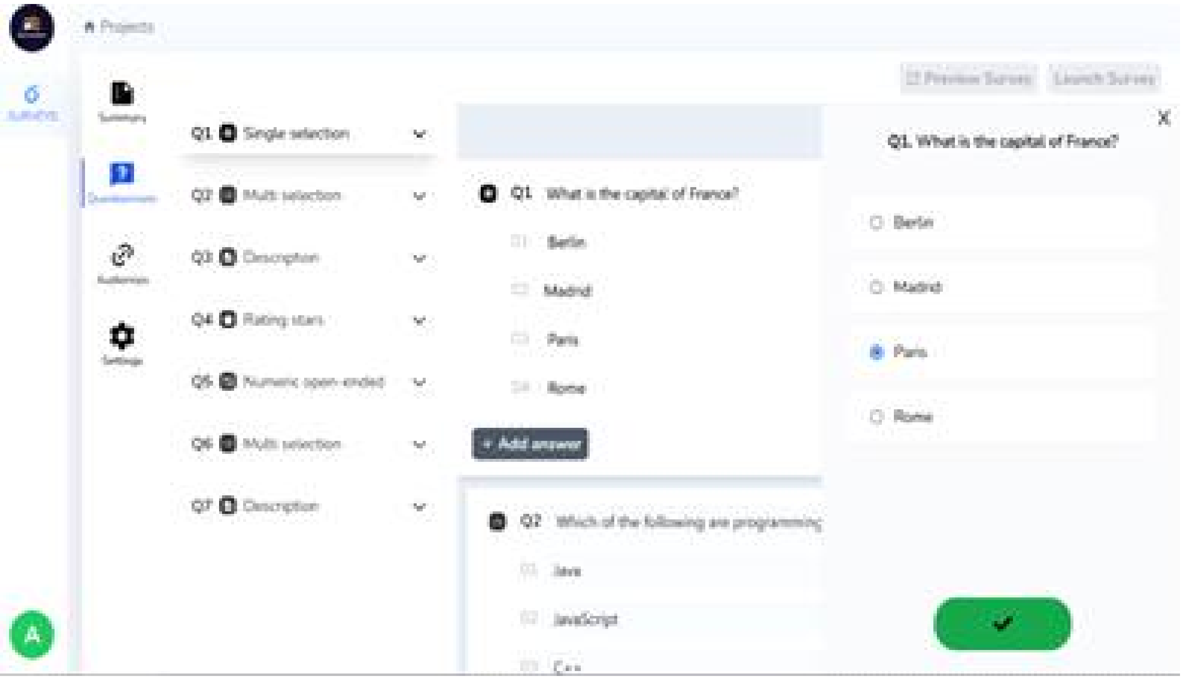
1.1 Application Interface

In the given figures 2-6, SurveyCraftapp interface is shown.



Don't have an account ?Signup

Fig.2: Sign-in Page



Q1 Single selection

Q2 Multi selection

Q3 Description

Q4 Rating stars

Q5 Numeric open-ended

Q6 Multi selection

Q7 Description

Q1 What is the capital of France?

01 Berlin

02 Madrid

03 Paris

04 Rome

Q2 Which of the following are programming

01 Java

02 JavaScript

03 C++

Q1. What is the capital of France?

○ Berlin

○ Madrid

● Paris

○ Rome

✓

Fig.3: Dashboard Page

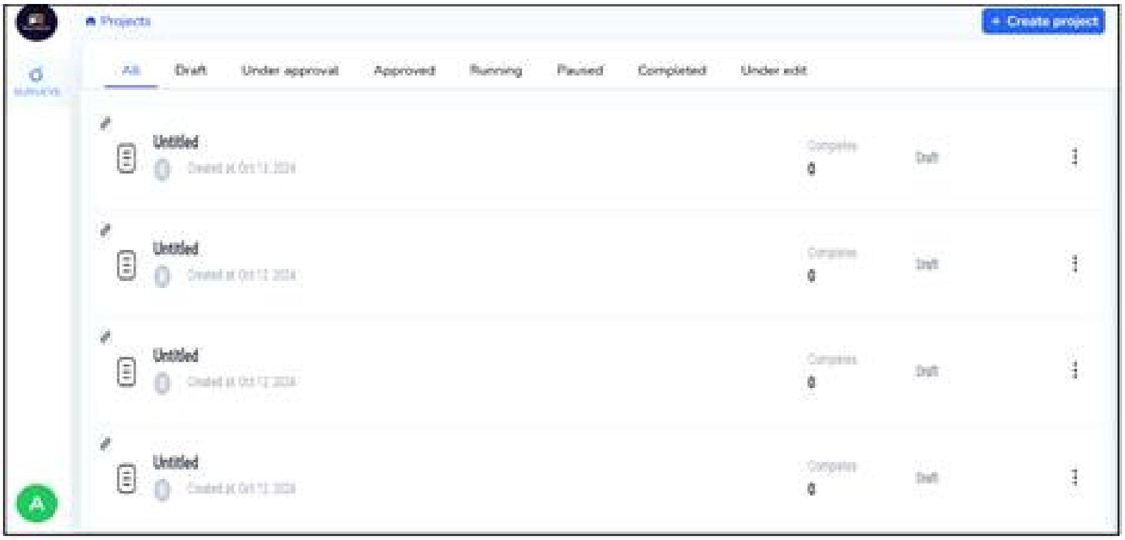


Fig.4: Survey Creation Page

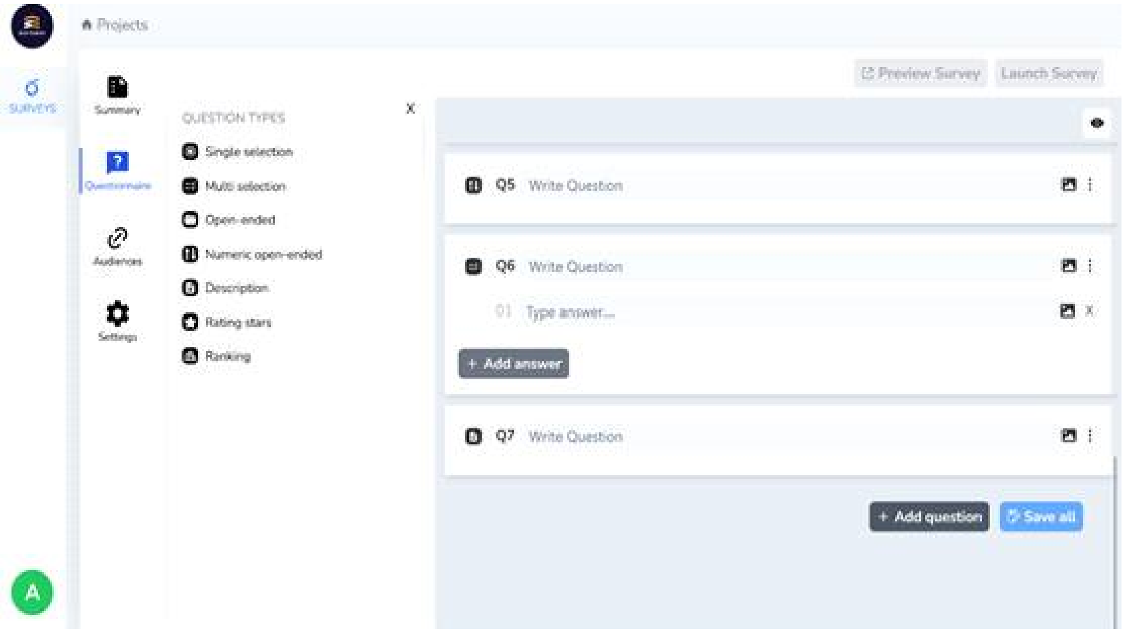
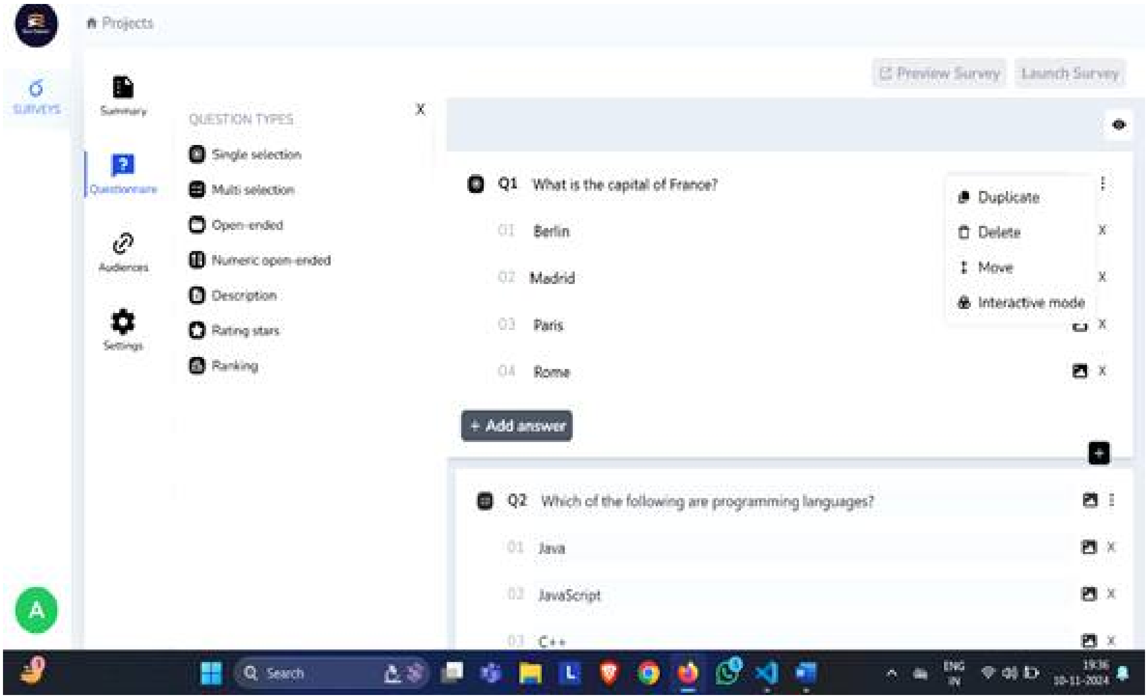


Fig.5: Add and Save



Q1 What is the capital of France?
01 Berlin
02 Madrid
03 Paris
04 Rome

Q2 Which of the following are programming languages?
01 Java
02 JavaScript
03 C++

Fig.6: Delete and more option

4. Findings

The development of the SurveyCraftapp with its set of features has resulted in a platform that efficiently handles survey creation, distribution, and response processing. Key findings include:

➢ High Response Rate Expectation: Based on the design, the platform is expected to handle surveys with a strong response rate, as the interface is intuitive and user-friendly.

➢ Diverse Question Types: The platform supports different types of questions, including single choice, multiple choicequestions (MCQs), and open-ended questions, allowing for comprehensive data collection.

➢ Real-Time Analytics: The survey feedback and results will no longer require waiting weeks for analysis as the system can process and visualize responses in one pipeline, providing feedback in under 10 mili-seconds.

➢ Error Handling: The platform incorporates error-checking mechanisms to address issues such as incomplete responses or network errors, minimizing disruptions in the survey participation process.

➢ Availability: The architecture is designed to keep surveys open at all times, and underwent availability testing over a period of time.

6. Conclusion and Future Scope

This paper discusses a proposed web-based survey creation applicationSurveyCrafta versatile and easy-to-use form builder to create one's own survey. It can handle multiple types of questions, including Likertscale with emojis, multiple choice, and open-ended questions, such that it's easy to create surveys and quiz that cover all bases. The app offers a clean interface, which enables creators to design and edit surveys with utmost ease. The platform focuses on ease of use, reliability, and flexibility to ensure smooth scaling.As this work discusses the initial release of the app with the general public, regular testing and updates will further help improve the performance of the application software.

References

1. Vitor Freitas. (2024). Django REST framework: The toolkit for building Web APIs. Retrieved from https://www.django-rest-framework.org

2. Django Software Foundation. (2024). Django documentation. Retrieved from https://www.djangoproject.com

3. React Team. (2024). React – A JavaScript library for building user interfaces. Retrieved from https://reactjs.org

4. Adam Wathan & Steve Schoger. (2024). Tailwind CSS - A utility-first CSS framework for creating custom designs. Retrieved from https://tailwindcss.com

5. Redis Documentation. Retrieved from: https://redis.io/docs/

6. JWT Authentication Tutorial. Retrieved from https://auth0.com/docs/secure/tokens/json-web-tokens

7. PostgreSQL Global Development Group. (2024). PostgreSQL: Documentation. Retrieved from https://www.postgresql.org/docs

8. Fowler, F. J. (2014). Survey Research Methods (5th ed.). SAGE Publications.

9. Williams, J. (2018). Web Development with Django: Learn to build powerful web applications using Python and Django. Packt Publishing.

10. Smith, J. (2023). The Rise of Digital Survey Tools in Business and Education. Tech Insights Journal.

11. Lee, Y., & Kim, J. (2021). Real-Time Analytics: A Key Component in Modern Survey Platforms. Data Science Review.

12. Brown, R., & White, S. (2023). Security Measures for Online Platforms: Ensuring Data Privacy in Survey Applications. Cybersecurity Today.

13. Patel, N., Kumar, S., & Shah, R. (2024). Scalable Solutions for Survey Platforms. Tech Engineering Review.

14. Chen, L. (2022). Background Task Processing in Web Applications. Web Development Journal.

15. Johnson, D. (2022). Survey Tools: Enhancing Data Collection in a Digital World. Business Technology Insights.

16. CeleryDocumentation. Retrieved from https://docs.celeryq.dev/en/stable/

17. Zhou, L., & Singh, M. (2018). Docker Containers: A Survey and Future Directions. International Journal of Computer Applications, 179(33), 36-43. Retrieved from https://www.ijcaonline.org/archives/volume179/number33/29447-2018910639

Innovations in Robotics, IoT, and Embedded Systems: Transforming Industries Through Smart Integration

Sushma Malik[1], Anamika Rana[2]
[1]Assistant Professor, [2]Associate Professor
Maharaja Surajmal Institute, New Delhi
[1]sushmalik25@gmail.com, [2]anamica.rana@gmail.com

Abstract: The convergence of Robotics, the Internet of Things (IoT), and Embedded Systems has revolutionized industries by enabling intelligent, autonomous, and connected solutions. Robotics provides automation capabilities, while IoT facilitates real-time data exchange, and Embedded Systems ensure efficient data processing and control. This integration has driven advancements in healthcare, manufacturing, agriculture, and smart cities. In healthcare, IoT-enabled robots support remote monitoring and precision surgeries. In manufacturing, smart factories leverage robotic arms equipped with IoT sensors for enhanced productivity and predictive maintenance. Agriculture benefits from automated irrigation systems and drones that optimize resource management. Smart cities employ these technologies to enhance public safety, traffic control, and environmental monitoring. Despite these advancements, challenges such as data security, system interoperability, and real-time processing limitations remain significant barriers to large-scale adoption. Future research should focus on developing robust communication protocols, improving AI-driven automation in robotics, and enhancing the energy efficiency of embedded systems. By addressing these challenges, the integration of Robotics, IoT, and Embedded Systems can unlock transformative potential, fostering smarter, safer, and more sustainable technological ecosystems.

Keywords: Robotics**,** Internet of Things (IoT), Embedded Systems, Autonomous Systems, Smart Cities, Industrial Automation, Real-Time Systems, Machine Learning

1. Introduction

The fields of Robotics, Internet of Things (IoT), and Embedded Systems have become pivotal in driving the digital transformation across industries. Each of these domains brings unique capabilities to the table, and their convergence is enabling the development of intelligent systems capable of automating complex tasks, collecting and processing data, and responding to real-time stimuli–[1].

- **Robotics:** Robotics is the study and creation of robots, which are machines designed to perform tasks automatically or with minimal human intervention. Robots can be used in various fields such as manufacturing, healthcare, agriculture, and service industries. They are often equipped with sensors, actuators, and advanced algorithms that enable them to perform tasks such as assembly, surgery, and even autonomous navigation[2].
- **Internet of Things (IoT):** IoT refers to the network of physical devices (like sensors, actuators, and other objects) that are interconnected and can communicate with each other over the internet. These devices can collect, exchange, and act on data without human intervention. For example, in smart homes, devices like thermostats, lights, and security cameras can be controlled remotely or programmed to work together to optimize energy use or enhance security[3].
- **Embedded Systems:** Embedded systems are specialized computing systems that are designed to carry out specific tasks. They are "embedded" within larger systems, meaning they aren't typically standalone computers but rather form part of a larger device. These systems are optimized for real-time operations and often have strict time constraints. Common examples include the control systems in cars (like anti-lock braking), medical devices (like pacemakers), and household electronics (like microwave ovens).The intersection of these technologies has given rise to new possibilities in areas like smart homes, smart cities, healthcare, industrial automation, and more. This paper aims to delve into these trends, highlight current applications, and discuss the future of robotics, IoT, and embedded systems integration[4].
- The combination of robotics, IoT, and embedded systems has led to the creation of intelligent systems. These systems can collect data, process it, make decisions, and perform actions autonomously or semi-autonomously, based on real-time data. This convergence enables the automation of complex tasks, such as remote monitoring of machinery, automated medical diagnoses, or even self-driving cars.

2. Integration of Robotics, IoT, and Embedded Systems

The integration of Robotics, Internet of Things (IoT), and Embedded Systems is creating powerful and efficient intelligent systems. These technologies work together to enable robots and devices to interact with the physical world, process data locally, and communicate with each other and the cloud. This section explores the connections between these fields and how they work together to create innovative solutions[5].

➢ **Robotics and IoT:**The integration of IoT with robotics significantly enhances the capabilities of robots. IoT enables remote monitoring and control of robotic systems, allowing them to interact with external devices and the environment[6]. Some of the key benefits and examples include:

➢ **Smart Manufacturing:** In smart manufacturing, robots are equipped with IoT sensors that can track equipment status in real-time. This provides valuable data for monitoring the health of machinery, which can be used to predict when maintenance is needed. This predictive maintenance helps prevent machine failure and minimizes downtime, improving productivity.

➢ **Autonomous Vehicles:** In the case of autonomous vehicles, IoT sensors (such as GPS, cameras, and radar) enable vehicles to interact with external devices like traffic signals, road sensors, and other vehicles. This exchange of data allows the vehicle to make decisions in real-time, improving its ability to navigate, avoid obstacles, and follow traffic laws without human intervention. The IoT infrastructure aids in the vehicle's autonomy by continuously collecting and sharing data from the vehicle's sensors to the cloud or local systems.

➢ **Collaborative Robots (Cobots):** Collaborative robots (or cobots) are robots designed to work alongside humans in a shared workspace. IoT allows these cobots to communicate with other machines and humans in real-time. This integration ensures that cobots can operate safely, adjust their actions based on human proximity, and collaborate efficiently with other machines. For instance, a cobot in a factory can communicate with other robots or devices to synchronize tasks, increasing efficiency and ensuring the safety of workers.

➢ **Embedded Systems in Robotics and IoT:**Embedded systems are the essential computing components that power both robotics and IoT devices. These systems are responsible for controlling, processing, and connecting devices, enabling them to function as part of a larger network. In robotics and IoT, embedded systems play key roles:

➢ **Processing:** Embedded systems are often designed to perform real-time computations. In robots, they control the motors, sensors, and actuators, ensuring that the robot responds to its environment and carries out tasks accurately and efficiently. In IoT devices, embedded systems process the data collected from sensors locally, reducing the need for cloud-based processing. This is crucial for applications requiring real-time response or where network connectivity is limited or unreliable.

➢ **Connectivity:** One of the most critical functions of embedded systems in IoT is enabling connectivity. They manage the communication between devices and the cloud. For example, embedded systems in an IoT-enabled robot allow it to send data about its status, environment, or performance to a central cloud server for further analysis. They also allow the robot to receive commands and updates from the cloud or other devices, making the robot a part of a larger interconnected system.

➢ **Control:** Embedded systems are responsible for the control of robots, especially in autonomous systems. In robotics, they determine the robot's actions based on input from sensors, cameras, and external devices. For instance, in autonomous vehicles, embedded systems control the vehicle's speed, direction, and responses to environmental changes, such as avoiding obstacles. In IoT, embedded systems manage the interactions between sensors and devices, enabling actions based on data inputs, like adjusting a thermostat based on temperature readings or triggering a security system when motion is detected.

3. Applications of Robotics, IoT, and Embedded Systems

The integration of Robotics, IoT, and Embedded Systems is transforming various industries by enabling more efficient, automated, and intelligent systems[7][6][8]. Below are some key areas where these technologies are having a significant impact:

3.1 Healthcare Robotic Surgery: IoT-enabled robots assist surgeons by providing precise, real-time data about the patient's condition, such as vital signs, tissue properties, and surgical tools' positions. This enhances the surgeon's capabilities, leading to more accurate procedures with smaller incisions and quicker recovery times. For example, robotic systems like da Vinci Surgical Systems offer advanced automation, allowing surgeons to perform minimally invasive procedures with high precision.

3.2 Remote Patient Monitoring: Wearable IoT devices (such as smartwatches or sensors) collect patient data, such as heart rate, blood pressure, glucose levels, or oxygen saturation. These devices are connected to embedded systems that process this data locally and send it to healthcare providers or the cloud for continuous monitoring. This allows for real-time health tracking, enabling early detection of medical issues and more timely interventions. Robots can also assist in administering medication, delivering supplies, or even helping patients with mobility.

3.3 Rehabilitation Robots: IoT and embedded systems are used to create rehabilitation robots that help patients recover from injuries or surgeries. These robots can track a patient's progress, such as range of motion or muscle strength, and adjust the rehabilitation program accordingly. Personalized rehabilitation programs can be designed based on the real-time data collected, leading to more effective and tailored recovery plans for each patient

4. Smart Homes and Cities

4.1 Smart Homes: In smart homes, robots, embedded systems, and IoT devices work together to automate and control various household systems like lighting, heating, cooling, security, and entertainment. For instance, robots can perform household chores like vacuuming (e.g., Roomba), cleaning windows, or even cooking meals. IoT devices (like smart thermostats and lights) enable remote control of the home environment through smartphones or voice assistants. Embedded systems control the operation of these devices, ensuring seamless interactions and energy-efficient performance.

4.2 Smart Cities: Robotics and IoT are applied in urban areas for managing resources and enhancing public safety. For example, robots can be used in waste management, performing tasks like collecting trash or sorting recyclables autonomously. IoT sensors are placed in various parts of the city to monitor traffic, pollution, energy use, and other metrics in real time. Embedded systems control urban infrastructure, such as traffic lights or street lighting, to optimize energy usage and reduce congestion.

➢ **Industrial Automation**

➢ **Automated Manufacturing:** In manufacturing, robotics and IoT come together to create intelligent factories. Robots equipped with IoT sensors gather data on machine performance, production rates, and product quality. This data is analyzed to improve the efficiency of production lines. Embedded systems control the operation of machinery, allowing for precise movements, adjustments, and automated quality checks. By connecting robots and machinery, manufacturers can streamline operations and reduce human error.

➢ **Predictive Maintenance:** IoT sensors embedded in industrial machines can monitor their health by tracking parameters like temperature, vibration, or pressure. This data is sent to robots or centralized systems, where embedded systems analyze it to predict when a machine will require maintenance. This predictive maintenance approach helps prevent unplanned downtime, extend the lifespan of machinery, and avoid costly repairs by addressing wear and tear before failure occurs.

➢ **Agriculture**

➢ **Precision Farming:** Robotic systems equipped with IoT sensors are used in precision farming to monitor crop health, soil conditions, and environmental factors in real time. These sensors gather data on soil moisture, temperature, and nutrient levels. Embedded systems process this data locally to optimize farming practices, such as adjusting irrigation schedules, fertilization, and pest control, leading to more efficient resource usage and higher crop yields.

➢ **Autonomous Tractors:** Autonomous tractors are robots that use IoT to navigate and perform agricultural tasks like plowing, planting, and harvesting. These tractors are equipped with GPS and other sensors, which allow them to operate autonomously in the fields, reducing the need for manual labor and increasing efficiency. Embedded systems control the navigation, movement, and task execution of the tractors, ensuring precision and minimizing resource waste.

5. Challenges and Limitations

Despite the transformative potential of integrating Robotics, IoT, and Embedded Systems across industries, several challenges hinder their seamless deployment and scalability[9][10][11]. Key challenges include:

➢ **Security and Privacy**

The integration of robotics, IoT, and embedded systems creates vast amounts of sensitive data. Ensuring secure communication and protecting against cyber-attacks are critical challenges, particularly in healthcare, industrial automation, and smart cities.

- **Interoperability**

IoT devices and robots often come from different manufacturers, each with its communication protocols and standards. Ensuring interoperability among these devices is crucial for seamless integration.

- **Real-Time Performance**

In robotics and IoT applications, systems often need to respond in real-time (e.g., autonomous vehicles or robotic surgery). Ensuring low-latency and high reliability in embedded systems remains a challenge.

- **Energy Efficiency**

Robotics and IoT devices often require continuous operation, but many of them have limited power supply. Energy-efficient embedded systems are crucial for prolonging the operation of battery-powered devices.

6. Future Directions

As these technologies continue to evolve, several key advancements and trends are expected to shape their future[10][12]:

- **Artificial Intelligence and Machine Learning**

Integrating AI and ML with robotics, IoT, and embedded systems will enable more autonomous and intelligent systems. For instance, robots can adapt to new environments, learn from experience, and improve performance over time.

- **Edge and Fog Computing**

By leveraging edge computing, which processes data closer to where it is generated, robotics and IoT systems can make faster, real-time decisions. Fog computing, a distributed computing model, is expected to become more prevalent in real-time applications such as autonomous vehicles and industrial automation.

- **5G Networks**

The advent of 5G technology will dramatically increase the data transmission speed and reduce latency, which is essential for supporting real-time, high-bandwidth applications in robotics, IoT, and embedded systems.

- **Quantum Computing**

Quantum computing may have a profound impact on embedded systems, enabling them to handle more complex computations. It could play a role in improving AI algorithms, particularly in real-time robotic control and decision-making.

7. Conclusion

The convergence of Robotics, IoT, and Embedded Systems holds immense potential to create smarter, more efficient, and more autonomous systems. By leveraging these technologies, industries such as healthcare, manufacturing, agriculture, and smart cities are witnessing transformative changes. However, challenges such as security, interoperability, real-time performance, and energy efficiency must be addressed to fully realize their potential. Moving forward, advances in AI, 5G, edge computing, and quantum computing will further enable the growth and sophistication of these systems, paving the way for a new era of intelligent automation.

References

1. O. Vermesan et al., “Internet of robotic things–converging sensing/actuating, hyperconnectivity, artificial intelligence and IoT platforms,” in Cognitive hyperconnected digital transformation, River Publishers, 2022, pp. 97–155.

2. R. Pugliese, S. Regondi, and R. Marini, “Machine learning-based approach: Global trends, research directions, and regulatory standpoints,” Data Sci. Manag., vol. 4, pp. 19–29, 2021.

3. K. Kuru and H. Yetgin, “Transformation to advanced mechatronics systems within new industrial revolution: A novel framework in automation of everything (AoE),” IEEE Access, vol. 7, pp. 41395–41415, 2019.

4. L. Romeo, A. Petitti, R. Marani, and A. Milella, “Internet of robotic things in smart domains: Applications and challenges,” Sensors, vol. 20, no. 12, p. 3355, 2020.

Legal Tackling of Cyber Crimes against Women in Prison

[1]Astha Bhatnagar, [2]Shewta Thakur
[1,2]Galgotias University
[1]asthaab716@gmail.com

Abstract: Cybercrimes against women have emerged as a critical issue in the digital era, with offenses like extortion, phishing, cyber stalking, and cyber defamation becoming increasingly common. This paper delves into the various forms of cybercrimes targeting women and evaluates the legal mechanisms designed to protect them. It examines key provisions of the Indian Penal Code, 1860, and the Information Technology Act, 2000, which address crimes such as sexual harassment, voyeurism, stalking, and identity theft. Additionally, the paper highlights significant judicial rulings that have influenced the legal framework for combating cybercrimes against women in India. By analyzing these legal provisions and landmark judgments, this study seeks to contribute to the development of more effective strategies for safeguarding women in the digital space.

Keywords: Cyber bullying, Cyber Crime, Information Technology Act, Phishing, Sextortion

1. Introduction

Cybercrime has become a pressing concern in the modern era, with women being among the most vulnerable targets. Cybercrimes refer to offenses committed through electronic communication or information systems, involving illegal activities where computers and networks play a central role. With the rapid expansion of the internet, the prevalence of cybercrimes has also surged, as criminals no longer require physical presence to commit offenses. In response to this growing threat, cyber laws were established to regulate and control crimes carried out via the internet, cyberspace, or digital resources. Cyber law encompasses legal issues related to the use of communication and computer technology, playing a crucial role in the digital age by governing online activities and transactions.

According to the National Crime Records Bureau (NCRB), 52,974 cases of cybercrime were registered, marking a 5.9% increase from 2020 (50,035 cases). The crime rate in this category rose from 3.7 in 2020 to 3.9 in 2021. In 2023, 60.8% of cybercrime cases were linked to fraud (32,230 out of 52,974 cases), followed by sexual exploitation at 8.6% (4,555 cases) and extortion at 5.4% (2,883 cases). The NCRB data for 2021 also revealed a more than 40% rise in crimes against women and children, a charge-sheeting rate of just 31% for IPC cases, and a staggering 111% increase in cybercrime cases in the national capital.

2. Types of Cyber Crimes Against Women

2.1 Sextortion: One of the most prevalent cybercrimes against women, even during the pandemic, was sextortion. Offenders blackmailed victims using their private or manipulated images, demanding money or sexual favors. Many perpetrators, frustrated by financial constraints, resorted to threats, coercing victims into engaging in video calls or exchanging explicit messages**.**

2.2 Phishing: Phishing is a fraudulent practice where an individual or entity impersonates a trusted organization in electronic communications, such as emails or messages, to deceive victims into revealing sensitive information like passwords and credit card details. It is a widespread form of cybercrime used to exploit personal and financial data**.**

2.3 Cyber Obscenity/Pornography: Considered one of the most severe online offenses, cyber obscenity involves the publication or distribution of pornographic content through electronic means. This includes the unauthorized dissemination of explicit material that violates privacy and dignity**.**

2.4 Cyber stalking: Women are often the primary targets of cyber stalking, a digital extension of traditional stalking. The Oxford Dictionary defines stalking as covertly pursuing someone. Cyber stalking includes tracking a person's online activities, sending persistent or threatening emails, posting messages on forums they frequent, or infiltrating their digital spaces. This crime leverages technology to harass and intimidate victims.

3. Legal Measures to Protect Women from Cybercrimes

Although there is no dedicated legal framework exclusively governing cybercrimes against women, several provisions across different laws offer legal recourse.

3.1 The Indian Penal Code (IPC), 1860

Before 2013, cyber bullying and online crimes against women were not directly addressed under the law. However, the **Criminal Law (Amendment) Act, 2013**, introduced Sections **354A to 354D** to tackle such offenses:

- **Sexual Harassment (Section 354A):**
- Covers acts such as demanding sexual favors, showing pornography without consent, or making sexually inappropriate remarks.
- Punishable by up to **three years of imprisonment, a fine, or both**.
- Less severe offenses carry penalties of up to **one year of imprisonment, a fine, or both**.

- **Voyeurism (Section 354C):**
- Defined as capturing or distributing images of a woman engaged in a private act without her consent.
- Conviction results in **up to three years of imprisonment for the first offense** and **up to seven years for repeat offenses**.

- **Stalking (Section 354D):**
- Covers both physical and online stalking, including persistently pursuing a woman despite her disinterest or monitoring her online activity.
- Punishable by **up to three years of imprisonment and a fine**, increasing to **five years for repeat offenses**.

- **Other Relevant Legal Provisions**

Beyond specific amendments, other sections of the IPC provide avenues for prosecuting cybercriminals:

- **Defamation (Section 499 & 500):**
- Intentionally harming someone's reputation through false statements or images.
- Punishable by **up to two years of imprisonment, a fine, or both**.

- **Criminal Intimidation (Section 503):**
- Threatening someone to manipulate or control their actions, often seen in cyber blackmail cases.

- **Anonymous Criminal Intimidation (Section 507):**
- Addresses threats made anonymously through digital means, providing for strict penalties.

- **Insulting a Woman's Modesty (Section 509):**
- Covers verbal remarks, gestures, or online content intended to offend or violate a woman's dignity.
- Offenders can face **up to three years of imprisonment and a fine**.

By enforcing these laws and raising awareness, stronger legal mechanisms can help curb cybercrimes against women and ensure their safety in the digital world.

3.2 The Information Technology Act, 2000

In order to facilitate electronic filing of documents with government agencies, this Act[16] was passed in 2000 to give legal recognition to transactions conducted through electronic data interchange and other electronic communication methods, also known as electronic commerce. These transactions incorporate the use of alternatives to paper-based methods of communication and information storage.

- **Offence of Identity Theft**: According to Section 66C of the IT Act, identity theft is a crime that carries penalties. This clause would apply to cyber hacking situations. This provision stipulates that anyone who dishonestly or fraudulently uses another person's password, electronic signature, or other unique identifying information faces a maximum sentence of three years in prison and a fine of up to Rs. one lakh.
- **Violation of Privacy:** Section 66E deals with situations in which someone's right to privacy is violated. Taking, sharing, or sending a picture of someone's private area without their permission or in a way that infringes on

their privacy can result in up to three years in prison and/or a fine.

➢ **Publishing or transmitting obscene material in electronic form:** Section 67, which prohibits the publication, transmission, or distribution of pornographic material, carries a maximum penalty of three years in prison or a fine for a first offense and up to five years in prison or a fine for a second.

➢ **Publishing or transmitting of material containing sexually explicit act, etc., in electronic form:** Section 67A defines publishing, transmitting, or assisting in the transfer of sexually explicit material as a misdemeanour, which carries a maximum sentence of five years in prison and a fine for a first conviction and a maximum sentence of seven years in prison and a fine for a subsequent conviction.

3.3 The Indecent Representation of Women Bill, 2012

Obscene depictions of women in publications, advertising, and other media are prohibited by this Bill. With the passage of this bill, the legal framework will be expanded to cover electronic and audio-visual media, as well as the distribution of information online and the representation of women on the internet. But as of July 2021, this Bill has been withdrawn.

4. Role of Indian Judiciary

The Indian judiciary has played a significant role in addressing cybercrime against women by delivering several landmark judgments. Some of these cases are highlighted below:

Ritu Kohli Case: The **Ritu Kohli Case** was India's first reported instance of **cyber stalking**. Mrs. Ritu Kohli filed a complaint with the police, stating that an individual was impersonating her online on for four consecutive days, primarily in the **Delhi Channel**. The impersonator used her name, shared her address, and engaged in inappropriate conversations. Furthermore, the individual intentionally provided her phone number to other chat participants, encouraging them to call her at odd hours.

As a result, Mrs. Kohli received nearly **40 calls** within three days, significantly disrupting her personal life. Following an investigation, the police traced the **IP addresses**, conducted a thorough inquiry, and arrested the offender. A case was filed under **Section 509 of the Indian Penal Code (IPC)**, but the accused was later released on bail. This case marked **India's first official report of cyber stalking**.

Cyber stalking, much like email harassment, is not explicitly addressed under existing **cyber laws in India**.
However, such offenses can be prosecuted under:

- **Section 72 of the Information Technology (IT) Act, 2000** – for breach of confidentiality and privacy.
- **Section 441 IPC** – for criminal trespass.
- **Section 509 IPC** – for outraging a woman's modesty.

This case set a precedent for recognizing **cyber stalking as a punishable offense**, highlighting the need for stronger legal provisions to tackle digital crimes.

In case of ***Avnish Bajaj* v. *State (N.C.T.) of Delhi***[1], Bazee.com a customer to customer website was caught selling MMS videos in the name "DPS girls having fun". Vanish bajaj CEO of the sales company was arrested and was his bail plea was rejected. He was arrested under section 67 of the Information Technology Act, 2000. In this case, the defendants claimed section 67 of Information Technology Act, 2000 relates to publication of obscene material not transmission of it. The court held that actual obscene recording/clip could not be viewed on the portal of Baazee.com.

A Chennai court rendered a decision in State of Tamil Nadu v. Suhas Katti[2] in 2004. After declining a man's marriage proposal, the divorced woman complained to the police about him sending her offensive, defamatory, and bothersome messages in a Yahoo message group. In order to forward emails received in the woman's name, the accused created a phony email account. People who thought the victim was soliciting for sex work also called her. After the police complaint was filed in February 2004, the Chennai Cyber Crime Cell was able to secure a conviction within seven months of the First Information Report being filed. Katti received two years of rigorous imprisonment and a fine of Rs. 500 for violating S. 469 IPC (forgery with the intent to damage one's reputation), one year of simple imprisonment and Rs. 500 for violating S. 509 IPC (words, gestures, or acts meant to offend a woman's modesty), and two years of rigorous imprisonment and a fine of Rs. 4,000 for violating S. 67 of the IT Act 2000 (punishment for publishing or transmitting obscene material in electronic form).

In ***Shreya Singhal* v. *Union of India*** [2], this ruling, which relates to section 66A of the Information Technology Act of 2000, is historic. This section was not part of the Act when it was first passed, but it was made effective on October 27, 2009, by an Amendment Act of 2009. "A rapid increase in computer and internet use has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism, breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personating commonly known as Phishing, identity theft, and offensive messages through communication services," the Amendment Bill explains in its justification for the insertion of section 66A. Therefore, in order to prevent such crimes, penal provisions must be incorporated into the Indian Penal Code, the Indian Evidence Act, the Information Technology Act, and the Code of Criminal Procedure.

5. Analysis of Present Legal System

The rising number of crimes against women is a significant concern for any state, but cybercrimes pose an even greater challenge due to the anonymity the internet provides. Criminals can easily create fake identities and engage in illegal activities, making detection and prosecution difficult. To combat this, the government should implement stricter regulations for **Internet Service Providers (ISPs)**, as they have complete access to data being used by individuals online. ISPs should be required to report any suspicious activities, which would help in preventing cybercrimes at an early stage.

Additionally, **cyber cafes** should be subject to stricter regulations, ensuring they maintain detailed records of customers who use their internet services. Many individuals engage in cybercrimes from cyber cafes to mask their identities and avoid detection. Proper record-keeping would make it easier for law enforcement agencies to track and identify offenders.

Public awareness regarding **cyber safety and digital rights** is also crucial. Many internet users in India are unaware of their rights and legal protections in cyberspace. Efforts must be made to educate people on how to safeguard themselves against cyber threats and ensure responsible digital behavior.

One of the major obstacles in addressing cybercrimes against women lies in **procedural legal challenges**, including jurisdictional conflicts, lack of sufficient evidence, and an underprepared judiciary. The judiciary plays a crucial role in shaping legal frameworks to combat cybercrimes effectively. With the expansion of cyberspace, traditional territorial boundaries have become less relevant. The jurisdictional limitations under **Section 16 of the Code of Civil Procedure and Section 2 of the Indian Penal Code** may not be sufficient to address cyber-related offenses, necessitating alternative dispute resolution methods for effective enforcement.

6. Conclusion

Several laws have been enacted to address cybercrimes against women, but continuous efforts are needed to ensure that technological advancements are used for ethical and legal purposes rather than criminal activities. Policymakers, law enforcement agencies, women's rights activists, and social organizations must recognize that cyberspace is as serious an issue as any other societal problem.

India, with its vast internet user base, faces a high risk of cybercrimes. Monitoring such a large digital landscape is challenging, and the government must **strengthen cyber security measures** to keep up with rapid developments in data services and internet access. In today's world, **cyber security is as critical as national security**, and building physical defenses will be ineffective if the real battle is being fought in the digital space. While global concerns over nuclear warfare persist, **cyber warfare has become an even more immediate and pressing issue**. India must ensure that women are not subjected to further victimization in this ever-evolving digital landscape.

References

1. Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on cyber crime and cyber laws of India.

International Research Journal of Engineering and Technology (IRJET), *4*(6), 1633-1640.

2. Balhara, Y. P. S., Sarkar, S., & Rajguru, A. J. (2024). Drug-related offences in India: Observations and insights from the secondary analysis of the data from the National Crimes Record Bureau. *Indian Journal of Psychological Medicine*, *46*(6), 527-534.

3. Rattan, J., & Rattan, V. (2017). Cyber Laws & Information Technology. *47 Bharat law publishing, Calcutta,*

4. GustafsonRID="**" ID="**" Present address: Courant Institute, 251 Mercer St., New York, NY 10012, USA.¶ E-mail: gustaf@ cims. nyu. edu, S., & Sigal, I. M. (2000). The Stability of Magnetic VorticesRID="*" ID="*" Research on this paper was supported by NSERC under grant N7901. *Communications in Mathematical Physics*, *212*(2), 257-275.

5. Ter-Akopian, G. M., Hamilton, J. H., Oganessian, Y. T., Daniel, A. V., Kormicki, J., Ramayya, A. V., ... & Saladin, J. X. (1996). New Spontaneous Fission Mode for 252 Cf: Indication of Hyperdeformed 1 4 4, 1 4 5, 1 4 6 Ba at Scission. *Physical review letters*, *77*(1), 32.

6. Ter-Akopian, G. M., Hamilton, J. H., Oganessian, Y. T., Daniel, A. V., Kormicki, J., Ramayya, A. V., ... & Saladin, J. X. (1996). New Spontaneous Fission Mode for 252 Cf: Indication of Hyperdeformed 1 4 4, 1 4 5, 1 4 6 Ba at Scission. *Physical review letters*, *77*(1), 32.

7. Law, U. (2009). *Indian Penal Code*. Universal Law Publishing.

8. Kushwah, J. P. (2021). Practical Approach towards Law Relating to Sexual Offences in perspective view of the Criminal Law (Amendment) Act, 2013. *Research Inspiration*, *7*(I), 15-23.

9. Dixit, V. A. I. B. H. A. V., & Singh, S. H. R. E. Y. (2013). The Criminal Law (Amendment) Bill, 2013-a Critical Analysis'. *Rostrum's Law Review*.

10. Kaur, D. R., & Aggarwal, D. R. A. (2013). The information technology act, 2000-demystified with reference to cybercrimes. *Paradigm*, *17*(1-2), 99-104.

A Comparative Study of Supervised and Unsupervised Machine Learning: Techniques, Applications, and Challenges

Abhinav Shukla[1], Sushma Malik[2], Anamika Rana[3]
[1]Belcan, Cognizant, USA, [2,3]Maharaja Surajmal Institute, New Delhi
[1]shuklaabhinav@yahoo.com,[2]sushmalik25@gmail.com, [3]anamica.rana@gmail.com

Abstract: Machine Learning (ML) is a rapidly evolving field that encompasses a wide range of techniques enabling computers to learn from data. Two of the most prominent paradigms in ML are Supervised Machine Learning (SML) and Unsupervised Machine Learning (UML), each suited to different problem types and requiring distinct approaches. This paper offers a comparative overview of these paradigms, focusing on their core concepts, key algorithms, evaluation metrics, and diverse applications. We discuss the challenges inherent to each approach—such as the need for labeled data in SML and the curse of dimensionality in UML—and explore emerging trends and future directions within both fields. By examining the strengths and limitations of SML and UML, this paper aims to underscore their complementary roles in addressing complex, real-world problems.

Keywords: Supervised Machine Learning (SML), Unsupervised Machine Learning (UML), Machine Learning paradigms, Algorithms, Data labeling, Evaluation metrics, Applications of ML, Emerging trends in ML, Classification, Clustering

1. Introduction

Machine Learning (ML) is a powerful subset of artificial intelligence (AI) that enables machines to automatically learn from data and improve over time without being explicitly programmed. In traditional programming, a developer writes specific rules and instructions to solve a problem. In contrast, in ML, the system learns patterns and insights directly from data. This ability to "learn" allows ML algorithms to adapt and generalize from examples, making them particularly suited for tasks where traditional rule-based systems might fall short or be impractical[1].
The Three Main Paradigms of Machine Learning:

Supervised Learning (SML): In Supervised Learning, the model is trained using a labeled dataset, where each data point comes with a corresponding target or output value. The goal is for the model to learn the mapping between input features and their associated labels so that it can predict the output for new, unseen data. Supervised Learning tasks are often categorized into classification (predicting discrete labels, such as whether an email is spam or not) and regression (predicting continuous values, such as house prices)[2].
Common algorithms: Linear Regression, Decision Trees, Support Vector Machines, Neural Networks, etc.

Unsupervised Learning (UML): In contrast to SML, Unsupervised Learning involves datasets that do not have labeled outcomes. The goal here is to find hidden structures or patterns in the data. The system tries to identify inherent groupings or correlations without any predefined outputs. For example, in clustering, a model might discover natural groupings of customers based on purchasing behavior without knowing the predefined categories.
Common tasks: Clustering (e.g., K-Means, DBSCAN), Dimensionality Reduction (e.g., PCA), Anomaly Detection, etc.

Reinforcement Learning (RL): While not the focus of your paper, it's worth noting that Reinforcement Learning is another key paradigm of ML. In RL, an agent learns by interacting with an environment and receiving feedback in the form of rewards or penalties. It's particularly useful for decision-making problems where the model has to take a series of actions to maximize cumulative reward (e.g., robotic control, game playing)[2].
In this paper, we are focusing specifically on the first two paradigms (Supervised and Unsupervised Learning), which have seen wide applications in various domains.

Why Focus on Supervised and Unsupervised Learning?
Supervised and Unsupervised Learning techniques have rapidly evolved and are integral to solving real-world problems, but they each come with distinct advantages and limitations. Let's delve deeper into why understanding these two paradigms is important[3][4].

➢ **Applications across Domains:**
Supervised Learning (SML): In fields like healthcare, SML is used for predictive modeling (e.g., diagnosing

diseases from medical images or predicting patient outcomes based on historical data). In finance, it's used for risk modeling, fraud detection, and credit scoring. The vast amount of labeled data available in these domains makes SML particularly powerful.

Unsupervised Learning (UML): In contrast, many applications lack labeled data, making UML an ideal solution. For example, marketing companies can use UML to segment customers into different groups based on purchasing behavior without needing predefined categories. Natural Language Processing (NLP) often uses UML techniques to uncover hidden semantic relationships in text data.

As more industries continue to digitize, the volume and complexity of data are increasing, and both SML and UML are critical in harnessing the potential of this data.

➢ **Challenges in Data Acquisition and Labeling:**

Supervised Learning's Data Dependency: One of the main limitations of SML is that it requires labeled data, which can be expensive, time-consuming, and labor-intensive to acquire. In real-world scenarios, labeling data requires domain expertise, and the lack of quality labels often limits the effectiveness of supervised models. For example, in healthcare, annotating medical images for supervised learning typically requires skilled radiologists.

Unsupervised Learning's Complexity and Ambiguity: While UML doesn't rely on labeled data, it comes with its own set of challenges. The algorithms often produce results that require human interpretation, and it's not always clear how to measure success (e.g., how to assess whether a clustering model has truly uncovered meaningful groups). Additionally, in high-dimensional data, unsupervised models can suffer from the "curse of dimensionality," where increasing data features make it harder to identify meaningful patterns.

➢ **Large Datasets and Increasing Complexity:** As datasets grow larger and more complex, SML and UML become increasingly important in tackling problems at scale. For example:

SML can be used to train models to predict outcomes based on large volumes of labeled data, which are becoming more common in fields such as autonomous driving, where systems are trained on vast amounts of sensor data.

UML plays a vital role when labeled data is scarce or unavailable, as it can extract insights from raw, unlabeled datasets, which are often the case in domains like social media analysis or big data analytics.

➢ **Adapting to Changing Data Environments:** Machine learning models need to evolve and adapt to new data over time. SML models may need to be retrained with new labeled data as patterns in the data change. Meanwhile, UML models, while not always requiring retraining with labeled data, can benefit from continual learning algorithms that help discover new structures as data evolves.

2. Fundamentals Of Supervised And Unsupervised Machine Learning

Supervised Machine Learning (SML) refers to a type of machine learning where the model is trained on a **labeled dataset**. Each input in the training set is paired with the correct output (label), allowing the algorithm to learn the mapping between the input features (predictors) and their corresponding output (target) values. The aim is for the model to predict the output for unseen, unlabeled data after training[5][6]. Table 1 shown the comparison and Table 2 represent the Key Algorithms and Techniques of SML and UML.

➢ **Training Data:** A labeled dataset consisting of input-output pairs (X, Y). Here, **X** represents the input features (e.g., pixels of an image, characteristics of a customer) and **Y** represents the corresponding output label (e.g., the class label for an image, the price of a house).

➢ **Learning Process:** The model tries to find a function or mapping $f:X \rightarrow Y$ that can generalize well to new, unseen examples.

➢ **Output:** The model is expected to predict an output value based on the learned function, either by **classification** (discrete output) or **regression** (continuous output).

Types of Supervised Learning:

➢ **Classification:** The task of predicting a discrete label or category for the input data. Common algorithms include:

➢ **Logistic Regression**

➢ **Decision Trees**

➢ **Random Forests**

➢ **Support Vector Machines (SVM)**

➢ **Neural Networks**

Example: Predicting whether an email is **spam** or **not spam** based on features like the presence of certain words.

- **Regression:** The task of predicting a continuous output. Common algorithms include:
- **Linear Regression**
- **Polynomial Regression**
- **Support Vector Regression (SVR)**
- **Decision Trees for Regression**

Example: Predicting the **price of a house** based on features like square footage, location, and number of rooms.

- **Key Elements in Supervised Learning:**
- **Features (X):** The input data or independent variables used to make predictions (e.g., age, income, etc.).
- **Labels (Y):** The desired output or dependent variable (e.g., disease diagnosis, customer purchase behavior, etc.).

Unsupervised Machine Learning (UML) involves training a model on **unlabeled data**—data that does not have predefined output labels. The goal of UML is not to predict specific outputs but to **identify patterns, structures, or relationships** within the data itself.

Since the data is unlabeled, the model's goal is usually to discover **hidden structures** or to reduce the complexity of the data (dimensionality reduction).

- **Training Data:** A dataset that contains input features but lacks corresponding output labels.
- **Learning Process:** The algorithm attempts to find underlying structure or patterns in the data, such as grouping similar instances together (clustering), finding important features (dimensionality reduction), or detecting anomalies.
- **Output:** The model typically outputs clusters, reduced dimensions, or associations rather than direct labels or values.
- **Types of Unsupervised Learning:**
- **Clustering:** The task of grouping similar data points together into clusters based on their features. The goal is to find natural groupings without prior knowledge of the data labels. Common algorithms include:
- **K-Means Clustering**
- **DBSCAN (Density-Based Spatial Clustering of Applications with Noise)**
- **Hierarchical Clustering**

Example: Grouping customers into segments based on purchasing behavior.

- **Dimensionality Reduction:** The task of reducing the number of features (or dimensions) in a dataset while retaining as much information as possible. Common techniques include:
- **Principal Component Analysis (PCA)**
- **t-Distributed Stochastic Neighbor Embedding (t-SNE)**
- **Autoencoders (in deep learning)**

Example: Reducing the dimensionality of gene expression data for visualization or further analysis.

- **Anomaly Detection:** Identifying rare or unusual instances that do not conform to the general pattern of the data. This can be useful for fraud detection, network security, etc. Common algorithms include:
- **Isolation Forest**
- **One-Class SVM**
- **K-Means (with outliers as a separate cluster)**

Example: Detecting fraudulent credit card transactions or network intrusions.

- **Key Elements in Unsupervised Learning:**
- **Features (X):** The input data (just like in SML) but without labels. Features could be anything from pixel values in images to transaction data in finance.
- **Clusters or Reduced Dimensions:** In clustering, the output will be a group of clusters that group similar data points together. In dimensionality reduction, the output will be a set of new features (principal components, for example) that capture the most important variance in the data.

Table 1: Comparisons of SML and UML[1][2]

Aspect	Supervised Learning (SML)	Unsupervised Learning (UML)
Data Requirement	Requires labeled data (input-output pairs)	Requires unlabeled data (only input data)
Goal	Learn a mapping from inputs to outputs (prediction)	Discover underlying patterns, structures, or relationships
Output	Predicted labels or continuous values	Groups, reduced dimensions, or anomaly scores
Types of Algorithms	Classification, Regression	Clustering, Dimensionality Reduction, Anomaly Detection
Evaluation Metrics	Accuracy, Precision, Recall, F1-score, MSE, R-squared	Silhouette Score, Davies-Bouldin Index, Variance Explained
Challenges	Need for large labeled datasets, overfitting, class imbalance	Difficulty in evaluation, interpretability, curse of dimensionality

Table 2: Key Algorithms and Techniques of SML and UML[1][2][7]

Paradigm	Algorithm/Technique	Core Functionality	Common Use Cases
Supervised Learning (SML)	**Linear Regression**	Predicts a continuous output variable based on input features using a linear approach.	Predicting house prices, stock market trends, or sales forecasting.
	Logistic Regression	A classification algorithm used to predict binary outcomes (0 or 1), estimating the probability of a certain class.	Email spam classification, medical diagnosis (e.g., cancer detection).
	Decision Trees	A tree-like model that splits the data based on feature values to predict discrete outcomes (classification) or continuous values (regression).	Customer segmentation, loan approval, predicting student performance.
	andom Forests	An ensemble of decision trees, used for both classification and regression. It aggregates the results of multiple trees to improve accuracy and avoid overfitting.	Fraud detection, medical diagnoses, stock market prediction.
	Support Vector Machines (SVM)	A powerful classifier that finds the hyperplane that best separates data into different classes. It can also be adapted for regression.	Image classification, text classification, bioinformatics.
	K-Nearest Neighbors (KNN)	A non-parametric algorithm that classifies new data points based on the majority class	Customer recommendation, anomaly detection, handwritten digit recognition.

		among its K-nearest neighbors in the feature space.	
	Naive Bayes	A probabilistic classifier based on Bayes' theorem, assuming independence between features.	Text classification (e.g., spam filtering), sentiment analysis.
	Neural Networks	Models that mimic the human brain, capable of learning complex patterns through layers of interconnected nodes. Can be used for both classification and regression.	Image recognition, speech recognition, natural language processing.
Unsupervised Learning (UML)	**K-Means Clustering**	Partitions data into K clusters by minimizing the variance within each cluster.	Customer segmentation, anomaly detection, market research.
	Hierarchical Clustering	Builds a tree-like structure (dendrogram) of nested clusters, useful for hierarchical relationships.	Gene expression analysis, social network analysis, customer segmentation.
	DBSCAN (Density-Based Spatial Clustering of Applications with Noise)	A clustering algorithm that groups points that are close to each other based on a density criterion. It can find clusters of arbitrary shape and identify outliers as noise.	Geospatial data clustering, image segmentation, noise filtering.
	Principal Component Analysis (PCA)	A dimensionality reduction technique that transforms features into a smaller set of linearly uncorrelated variables (principal components).	Image compression, exploratory data analysis, noise reduction.
	Gaussian Mixture Models (GMM)	A probabilistic model that assumes that the data is generated from a mixture of several Gaussian distributions.	Anomaly detection, image segmentation, density estimation.
	Independent Component Analysis (ICA)	A technique for separating a multivariate signal into additive, independent components. Used when the assumption is that the signals are statistically independent.	Signal processing, image separation, EEG signal analysis.

3. Evaluation Metrics And Performance Assessment

In machine learning, performance evaluation is critical for understanding how well a model is performing, and selecting the best model for deployment. For Supervised Learning (SML) and Unsupervised Learning (UML), there are distinct sets of evaluation metrics tailored to the nature of each paradigm—[8]. Some evaluation metrics and performance assessment form are sown in table 3.

Table 3: Evaluation Metrics and Performance Assessment of SML and UML—[8][9]

Metric	Type	Purpose	Use Case
Accuracy	SML	Measures the percentage of correct predictions.	When classes are balanced.
Precision	SML	Measures the accuracy of positive predictions.	Imbalanced data, when false positives are costly.
Recall	SML	Measures the ability to find all relevant positive instances.	Imbalanced data, when false negatives are costly.
F1-Score	SML	Balances precision and recall.	Imbalanced data, when both false positives and false negatives matter.
Confusion Matrix	SML	Detailed breakdown of true/false positives/negatives.	Assessing classification model performance.
ROC Curve & AUC	SML	Evaluates performance at various thresholds.	Binary classification, especially with imbalanced data.
Silhouette Score	UML	Measures clustering quality.	Evaluating clustering algorithms.
Davies-Bouldin Index	UML	Measures cluster separation.	Comparing clustering algorithms.
Cluster Purity	UML	Measures how pure clusters are in terms of the class labels.	Semi-supervised learning, clustering tasks.
Variance Explained (PCA)	UML	Measures the proportion	

4. Applications of Supervised and Unsupervised Learning

Supervised learning excels in prediction and classification tasks like disease diagnosis, credit scoring, and spam detection. Unsupervised learning identifies patterns in unlabeled data, aiding in customer segmentation, anomaly detection, and recommendation systems. Both techniques are vital in enhancing AI-driven solutions across industries such as healthcare, finance, and marketing[10]. Table 4 represents the Summary of Applications of SML and UML.

Table 4: Summary of Applications of SML and UML[10][11]

Supervised Learning Applications	Unsupervised Learning Applications
Healthcare: Disease diagnosis, patient risk prediction	**Customer Segmentation:** Grouping customers for targeted marketing
Finance: Fraud detection, credit scoring	**Anomaly Detection:** Fraud detection, network intrusion
E-commerce & Marketing: Customer segmentation, recommendation systems	**Dimensionality Reduction:** Data simplification, visualization
Autonomous Vehicles: Object detection, traffic sign recognition	**Generative Models:** Synthetic data generation, data augmentation
Stock Market Prediction: Predicting trends and prices	

5. Challenges in Supervised and Unsupervised Learning

Machine learning techniques, including **Supervised Learning (SL)** and **Unsupervised Learning (USL)**, come with their own set of challenges. These challenges can impact model performance, scalability, and real-world applicability[12]. Below table 5 explore the key challenges faced in both paradigms:

Table 5: Summary of Key Challenges[12][13]

Supervised Learning Challenges	Unsupervised Learning Challenges
Data Labeling: Time-consuming and expensive to label data.	**Lack of Ground Truth:** Difficult to evaluate model quality without labeled data.
Overfitting: Models may memorize the training data.	**Curse of Dimensionality:** High-dimensional data makes it hard to find meaningful patterns.
Imbalanced Data: Model may be biased toward the majority class.	**Choosing the Right Algorithm:** Selecting the appropriate algorithm for high-dimensional or complex data.
Model Interpretability: Complex models can be difficult to interpret.	**Interpretability:** Unsupervised results may be abstract and hard to understand.

6. Emerging Trends and Future Directions

The future of **Supervised Learning (SML)** and **Unsupervised Learning (USL)** is poised for significant advancements, driven by innovations like **Semi-Supervised Learning**, **Transfer Learning**, and **Explainable AI (XAI)**. These trends promise to address current challenges such as data scarcity, model interpretability, and privacy concerns as shown in table 6. Furthermore, **Deep Learning** and **Federated Learning** will continue to push the boundaries of what is possible, enabling more personalized, privacy-preserving, and efficient machine learning systems across a range of applications. As these trends mature, they will enable more scalable, adaptable, and trustworthy AI solutions for complex, real-world problems[14].

Table 6: Summary of Emerging Trends[14][15]

Trend	Description	Key Applications
Semi-Supervised Learning (SSL)	Combines labeled and unlabeled data to improve performance with fewer labels.	Healthcare (medical image analysis), Speech Recognition, NLP
Transfer Learning	Leverages pre-trained models on large datasets to enhance learning in new tasks.	Image Recognition, NLP, Speech Processing
Explainable AI (XAI)	Makes AI models interpretable, transparent, and explainable for trust and compliance.	Healthcare, Finance, Legal, Autonomous Vehicles
Deep Learning & Unsupervised Representation Learning	Advances in unsupervised learning methods like autoencoders and GANs for feature learning and data generation.	Anomaly Detection, Image Generation, Data Augmentation
Federated Learning	Decentralized model training on local devices while preserving privacy.	Healthcare, Mobile Devices, IoT, Financial Services

7. Conclusion

Supervised Machine Learning (SML) and Unsupervised Machine Learning (UML) are key approaches in solving real-world problems. SML leverages labeled data for tasks like classification and regression, excelling in healthcare, finance, and e-commerce. However, it requires extensive labeled data and faces risks like overfitting. Conversely, UML identifies patterns in unlabeled data, ideal for clustering, anomaly detection, and data compression. Despite its versatility, UML lacks clear evaluation metrics due to the absence of ground truth. Combining these approaches through techniques like semi-supervised learning and transfer learning enhances model performance. Emerging trends like federated learning and deep learning continue to improve both methods.

References

1. K. Makkar, P. Kumar, M. Poriye, and S. Aggarwal, “A comparative study of supervised and unsupervised machine learning algorithms on consumer reviews,” in 2022 IEEE World Conference on Applied Intelligence and Computing (AIC), 2022, pp. 598–603.

2. A. K. Hamoud et al., “A comparative study of supervised/unsupervised machine learning algorithms with feature selection approaches to predict student performance,” Int. J. Data Mining, Model. Manag., vol. 15, no. 4, pp. 393–409, 2023.

3. R. Sharma, K. Sharma, and A. Khanna, “Study of supervised learning and unsupervised learning,” Int. J. Res. Appl. Sci. Eng. Technol., vol. 8, no. 6, pp. 588–593, 2020.

4. T. Hodel, “Supervised and unsupervised: approaches to machine learning for textual entities,” Digit. Humanit. Res. Vol. 2, p. 157, 2022.

5. K. Sindhu Meena and S. Suriya, “A survey on supervised and unsupervised learning techniques,” in Proceedings of international conference on artificial intelligence, smart grid and smart city applications: AISGSC 2019, 2020, pp. 627–644.

6. T. Talaei Khoei and N. Kaabouch, “Machine learning: Models, challenges, and research directions,” Futur. Internet, vol. 15, no. 10, p. 332, 2023.

7. K. K. Verma, B. M. Singh, and A. Dixit, “A review of supervised and unsupervised machine learning techniques for suspicious behavior recognition in intelligent surveillance system,” Int. J. Inf. Technol., vol. 14, no. 1, pp. 397–410, 2022.

8. C. Esther Varma and P. S. Prasad, “Supervised and Unsupervised Machine Learning Approaches—A Survey,” in ICDSMLA 2021: Proceedings of the 3rd International Conference on Data Science, Machine Learning and Applications, 2023, pp. 73–81.

9. I. H. Sarker, “Machine learning: Algorithms, real-world applications and research directions,” SN Comput. Sci., vol. 2, no. 3, p. 160, 2021.

10. M. Usama et al., “Unsupervised machine learning for networking: Techniques, applications and research challenges,” IEEE access, vol. 7, pp. 65579–65615, 2019.

11. A. Sharma, A. Kaur, and A. Semwal, “Supervised and unsupervised prediction application of machine learning,” in 2022 International Conference on Cyber Resilience (ICCR), 2022, pp. 1–5.

12. M. T. Almuqati, F. Sidi, S. N. Mohd Rum, M. Zolkepli, and I. Ishak, “Challenges in Supervised and Unsupervised Learning: A Comprehensive Overview.,” Int. J. Adv. Sci. Eng. Inf. Technol., vol. 14, no. 4, 2024.

13. M. Alloghani, D. Al-Jumeily, J. Mustafina, A. Hussain, and A. J. Aljaaf, “A systematic review on supervised and unsupervised machine learning algorithms for data science,” Supervised unsupervised Learn. data Sci., pp. 3–21, 2020.

14. N. Rane, S. Choudhary, and J. Rane, “Machine learning and deep learning: A comprehensive review on methods, techniques, applications, challenges, and future directions,” Tech. Appl. Challenges, Futur. Dir. (May 31, 2024), 2024.

15. R. Pugliese, S. Regondi, and R. Marini, “Machine learning-based approach: Global trends, research directions, and regulatory standpoints,” Data Sci. Manag., vol. 4, pp. 19–29, 2021.

IITM Journal of Information Technology

Paper Submission Guidelines

Submission of Paper is in Two Stages:

1. **Initial Paper Submission:** Prospective Author(s) is / are encouraged to submit their Manuscript including Charts, Tables, Figures and Appendixes in .pdf and .doc (both) Strictly using single column Springer format to itjournal@iitmjp.ac.in

All submitted articles must present original, previously unpublished research findings, whether experimental or theoretical. Articles should adhere to these criteria and must not be simultaneously under consideration for publication.

2. **Camera Ready Paper Submission:** After the completion of the review process, Author(s) are required to submit the camera-ready full-text paper in both .doc and .pdf formats upon paper acceptance.

***THERE IS NO PUBLICATION FEE**

Institute of Innovation in Technology and Management

Affiliated to GGSIPU, NAAC Grade 'A',
ISO 14001:2015, 17020:2012, 21001:2018 & 50001:2018 Certified,
A Grade by GNCTD, A Grade by SFRC

D-27/28, Institutional Area, Janakpuri, New De1hi-110058
Tel: 011-28520890, 28520894
E-mail: director@iitmjp.ac.in Website: http://www.iitmjp.ac.in