DEPARTMENT OF BIOMEDICAL ENGINEERING

24AI671-FUNDAMENTALS OF DATA SCIENCE

UNIT V- DATA SCIENCE FOR REAL-WORLD ENGINEERING SOLUTIONS

4. AI-POWERED DECISION SUPPORT SYSTEMS (DSS)

A **Decision Support System (DSS)** is an interactive computer-based system that helps managers and engineers take decisions by using **data, models and knowledge**. It is mainly used for problems that are semi-structured or unstructured, where no single fixed answer exists.

An **AI-powered DSS** adds artificial intelligence – machine learning, natural language processing, expert systems and optimisation – to the traditional DSS. It can learn from data, predict outcomes, explain its reasons and suggest actions in real time. The important point is that it **supports** the human decision-maker; the **final decision is still taken by the human**.

Architecture and Components

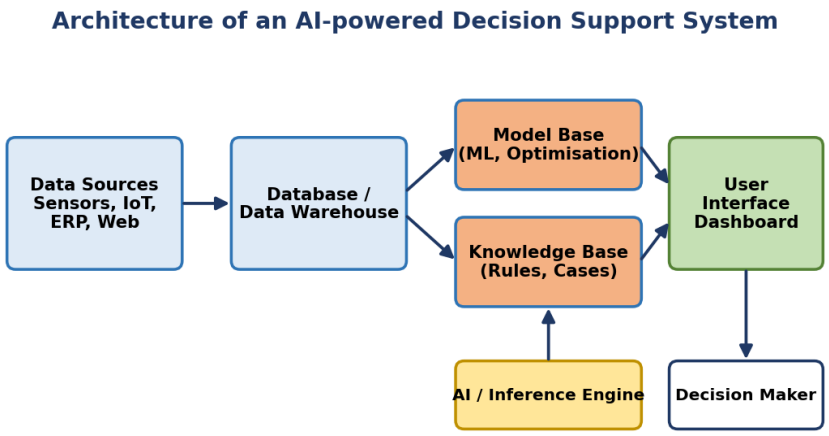


Fig 4.1 Architecture of an AI-powered DSS

Data from many sources is stored in the database, the AI models and knowledge base process it, and the results are shown to the user through an interface.

Component	Function
Data sources	Sensors, IoT devices, ERP, web data and company records that supply raw data
Database / Data warehouse	Stores, organises and manages the collected data
Model base	Collection of statistical, machine learning, optimisation and simulation models
Knowledge base	Expert rules, facts and past cases of the problem area
AI / Inference engine	Applies the models and rules to the data to produce predictions and recommendations
User interface	Dashboards, charts, alerts and natural-language or voice queries for the user
Explanation module	Shows why a recommendation was made, so the user can trust it

Types of DSS

Type	Based On	Example
Data-driven	Access and analysis of large data sets	Sales or production dashboard
Model-driven	Mathematical, optimisation or simulation models	Production scheduling tool
Knowledge-driven	Expert rules and reasoning	Fault-diagnosis expert system
Communication-driven	Group discussion and collaboration	Online meeting and shared-board tools
Document-driven	Text, reports and documents	Technical document search engine

AI Techniques Used in DSS

- **Machine learning** – predicts outcomes, classifies data and detects abnormal behaviour.
- **NLP and chatbots** – let users ask questions in simple language and get summarised reports.
- **Expert systems and fuzzy logic** – make decisions using rules and handle uncertain or vague information.
- **Optimisation and reinforcement learning** – select the best action among many choices.
- **Computer vision** – analyses images and video, for example for quality inspection.

- **Digital twin** – a virtual model of a real system that is used to test decisions safely before applying them.

How It Works

- Data is collected from many sources and integrated in the database.
- AI models analyse the data and generate predictions and alternative solutions.
- The alternatives are ranked and shown on the dashboard with explanations.
- The human decision-maker reviews the suggestions and takes the final decision.
- The result of the decision is stored and fed back, so that the system keeps learning.

Applications

- **Manufacturing** – maintenance scheduling, quality control and production planning.
- **Healthcare** – clinical decision support to help doctors in diagnosis and treatment.
- **Agriculture** – advice on crop selection, irrigation and fertiliser using soil and weather data.
- **Smart grid and energy** – load balancing and power dispatch decisions.
- **Smart city and transport** – traffic signal control and route planning.
- **Finance and supply chain** – credit scoring, fraud detection and inventory planning.

Benefits and Challenges

Benefits	Challenges
Fast, accurate and consistent decisions	Poor data quality gives wrong advice

Benefits	Challenges
Handles large and complex data easily	Black-box AI models reduce trust and understanding
Reduces human error and cost	High setup cost and need for skilled people
Works 24×7 in real time	Bias, privacy and security risks

5.5. DATA ETHICS, PRIVACY, BIAS AND SECURITY

Data science and AI now influence important areas of life such as jobs, loans, healthcare, policing and safety. If data is misused or a model is unfair, real people can be harmed. **Data ethics** is the set of moral principles that guide how data is **collected, stored, analysed, shared and used**. Its four major concerns are ethics, privacy, bias and security.

Data Ethics – Core Principles

- **Transparency** – people should be told clearly what data is collected and how it is used.
- **Informed consent** – data is collected only after the person gives clear permission, and they can withdraw it.
- **Fairness** – the results should not discriminate against any person or group because of gender, caste, religion, age or region.
- **Accountability** – the organisation and the developers are responsible for the results and effects of their models.
- **Data minimisation and purpose limitation** – only the data that is really needed is collected, and it is used only for the stated purpose.
- **Beneficence** – data should be used for the benefit of individuals and society and should not cause harm.

Data Privacy

Privacy is the right of a person to control how their personal data is collected, stored and used. **PII (Personally Identifiable Information)** is any data that can identify a person, such as name, Aadhaar number, phone number, email, address, photograph, biometrics and location. Sensitive data such as health, financial and political details needs extra protection.

Privacy Laws

Law	Region	Key Points

Law	Region	Key Points
GDPR (2018)	European Union	Consent, right to access and correct data, right to be forgotten, data portability, very heavy penalties
Digital Personal Data Protection (DPDP) Act, 2023	India	Consent-based processing of personal data, rights of individuals (data principals), duties of organisations (data fiduciaries), penalties for breach
Information Technology Act, 2000	India	Legal recognition of electronic records; provisions for cyber-crime and data protection
HIPAA / CCPA	USA	Protection of health data (HIPAA) and consumer data rights in California (CCPA)

Privacy-Preserving Techniques

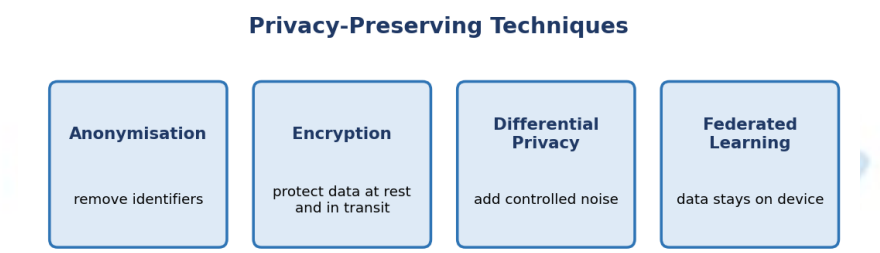


Fig 5.1 Privacy-preserving techniques

- **Anonymisation and pseudonymisation** – names and identity details are removed or replaced with codes so the data cannot be linked to a person.

- **Data masking and generalisation** – sensitive fields are hidden, or exact values are replaced by ranges (for example age 34 becomes 30–40).
- **Encryption** – data is converted into unreadable form while stored (at rest) and while being sent (in transit) using AES, RSA and TLS.
- **Differential privacy** – a small amount of random noise is added to the data or results, so the presence of any single person cannot be identified.
- **Federated learning** – the model is trained on the user's own device and only the model updates are shared; the raw data never leaves the device.

Bias in Data and Algorithms

Bias is a systematic error that gives unfair or inaccurate results for some people or groups. A biased model can reject deserving candidates, give wrong medical results or increase existing inequality. Bias can enter in the data, in the algorithm or through human decisions.

Type of Bias	Meaning	Example
Sampling / Selection bias	Training data does not represent the whole population	Face data with mostly one skin tone gives poor results for others
Historical bias	Data reflects past social inequality	Old hiring data that favours one gender
Measurement bias	Faulty or inconsistent data collection	Poorly calibrated sensors
Label bias	Wrong or subjective labels given by humans	Inconsistent tagging of images

Type of Bias	Meaning	Example
Algorithmic bias	The model design favours some outcomes	Loan model using pincode as a proxy for caste or income
Confirmation bias	Looking only for results that support one's belief	Ignoring results that contradict the expectation

Reducing Bias

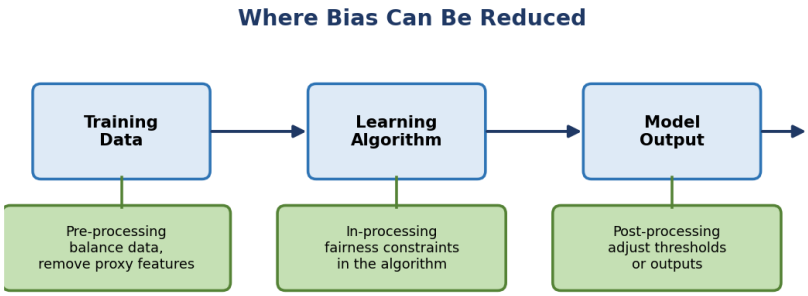


Fig 5.2 Bias mitigation at three stages

- **Pre-processing** – collect balanced data, re-sample the data and remove features that act as proxies for sensitive attributes.
- **In-processing** – add fairness conditions inside the learning algorithm so it is penalised for unfair results.
- **Post-processing** – adjust the model's outputs or decision thresholds for different groups.
- Measure fairness with **demographic parity** (equal selection rate for groups) and **equal opportunity** (equal true-positive rate), and conduct regular bias audits using diverse teams.

Real example: An automated recruitment tool trained on ten years of past resumes learned to prefer male candidates, because the earlier hiring was male-

dominated. The tool was withdrawn – showing how historical bias is repeated by AI.

Data Security

Data security means protecting data from unauthorised access, theft, loss or damage. It is based on the **CIA triad** – Confidentiality (only authorised people can see data), Integrity (data is accurate and not changed illegally) and Availability (data is available when needed).

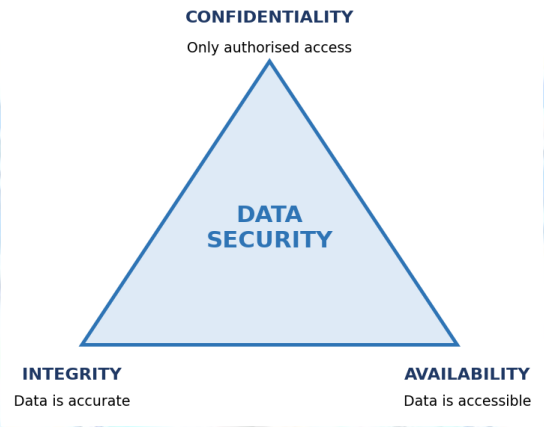


Fig 5.3 CIA triad

Common Threats

Threat	Meaning
Data breach / hacking	Unauthorised access to confidential data
Malware / ransomware	Harmful software that steals data or locks it for ransom
Insider threat	Misuse of data by employees or contractors
Adversarial attack	Specially altered inputs that make an ML model give wrong output

Threat	Meaning
Data poisoning	Adding false data to the training set to spoil the model
Model inversion / theft	Recovering private training data or copying the model through repeated queries

Security Controls

- Strong authentication (multi-factor) and role-based access control, so people see only the data they need.
- Encryption of data, secure key management, firewalls and intrusion-detection systems.
- Regular backup, software updates and patching, audit logs and security testing.
- A secure ML pipeline – validates input data, monitor models for attacks and restrict API access.
- Staff training and a ready incident-response plan.