Challenges In Mobile App Security
&
Types Of Wireless Attacks

UNIT IV

R DEVIKA

Overview

- Challenges in mobile app security
- Tools for mobile automation testing
- Weak encryptions
- Weak hosting controls
- Insecure data storage

Mobile application testing is a complex and challenging task

1. Mobile application testing needs to cover multiple devices with different capabilities and limitations.
2. Testing on each version of the operating system is time-consuming and requires testers to be aware of the loopholes.
3. Each device has its own unique set of hardware and software configurations, which can impact the security of the mobile application.
4. When the testing team becomes a bottleneck in the release process, it can lead to the production of low-quality apps.
5. The testing team may not be able to thoroughly test the app due to time constraints or other factors, which can result in undetected security vulnerabilities and other issues that can impact the user experience.
6. Mobile application testing is a critical component of the development process.
7. Organizations need to invest in the necessary resources and tools to ensure that their apps are thoroughly tested and of high quality

Mobile automation testing tool

1. Traditional testing tools like Selenium or QuickTest Professional (QTP) may not be suitable for **mobile automation testing**.
2. Mobile automation testing requires different tools that can cater to the specific challenges of testing on **multiple devices with different configurations**.
3. There is a lack of **full-fledged standard tools** that can handle every aspect of the **security testing process**.
4. Common mobile automation testing tools include **Appium, Robotium, and Ranorex**.
5. These tools are **specifically designed for mobile testing** and can help with various aspects of the testing process, including **security testing**.
6. Testing teams should **explore and use the appropriate mobile automation testing tools** that can cater to the specific needs of their testing requirements.
7. Using the right mobile automation testing tools can ensure that mobile apps are **thoroughly tested and of high quality**.

Steps Involved in a Comprehensive Testing Strategy	Description
1. Identify potential risks	Identify potential risks that could impact the security of the mobile app, including device fragmentation, weak encryption, and insecure data storage.
2. Design test cases	Design test cases to assess the security of the mobile app, including testing the app's code for vulnerabilities and testing its behavior under different conditions.
3. Implement test cases	Implement the designed test cases by testing the mobile app under various conditions, including different devices, operating systems, and network configurations.
4. Analyze results	Analyze the testing results to identify any vulnerabilities or weaknesses in the mobile app's security, including device fragmentation, weak encryption, and insecure data storage.
5. Address vulnerabilities	Address any vulnerabilities identified in the testing phase by modifying the mobile app's code, improving encryption, or implementing more secure data storage solution

Weak encryption

- Encryption is essential in mobile app security to safeguard sensitive data and prevent unauthorized access.
- Inadequate encryption can enable attackers to modify cookies and environment variables, bypassing authentication and authorization decisions based on them.
- Examples of weak encryption include the **Starbucks mobile app storing** usernames, email addresses, and passwords in plain text.
- Weak encryption makes it easier for attackers to access sensitive information and compromise user account security.
- App developers need to implement strong encryption practices to protect sensitive data from potential attacks.
- Strong encryption practices can involve using encryption algorithms like AES, implementing secure communication protocols like SSL/TLS, and regularly updating encryption keys to prevent potential vulnerabilities

Weak hosting controls

1. lack of security measures or procedures in place to protect a website or server from potential security threats.
2. small business is developing their first mobile application for online purchases.
3. To host the app and store customer data, the business creates a new server.
4. Without proper security measures in place, the server and customer data may be vulnerable to attacks from outside networks.
5. Hackers could gain unauthorized access to the data and use it for malicious purposes.
6. To prevent this, the business needs to implement proper security measures such as firewalls, secure login processes, and regular security updates.
7. Back-end services should also be secured against malicious attacks and accessed only by authorized personnel.
8. By taking these steps, the business can protect their customer data and prevent potential security breaches.
9. This can help build trust with customers who know their sensitive information is safe and secure

key measures for ensuring good hosting controls

1. Regular security updates and patches: Regularly applying security updates and patches to web servers, content management systems (CMS), and other software applications can help prevent vulnerabilities from being exploited by hackers.
2. Strong passwords: Using strong, unique passwords that are difficult to guess or crack can help prevent unauthorized access to the website or server.
3. Access controls: Implementing access controls, such as two-factor authentication or restricted access permissions, can help ensure that only authorized users have access to sensitive data or can make changes to the website.
4. Backups: Regularly backing up website data can help ensure that data can be restored in the event of a security breach or other disaster.
5. Firewall protection: Implementing a firewall can help prevent unauthorized access to the website or server by blocking malicious traffic.
6. Monitoring: Regularly monitoring website and server activity can help detect potential security threats and prevent them before they can cause damage.

Insecure data storage

- In mobile app security, it's important to ensure **that user data is kept secure**. This includes **encrypting critical information** such as contact details, passwords, and credit card numbers.
- To minimize the risk of data breaches, apps should be designed in such a way that critical information is not stored directly on a device. If it is stored on the device, it must be done securely.— indirectly stored on cloud and E2EE
- Examples of insecure data storage include a flaw in Skype data security, which allowed hackers to dial arbitrary phone numbers using a simple link in the contents of an email.
- To prevent these kinds of security vulnerabilities, app developers should implement strong encryption practices and follow secure coding best practices. This can help protect sensitive user data and prevent potential security breaches

Types of wireless attacks

- Packet sniffing
- Rogue access point
- Password theft
- Man-in-the-middle attack
- Jamming
- War driving
- Bluetooth attacks
- WEP/WPA attacks

- Packet sniffing:
- Traffic is sent in packets over a network.
  - When data is sent over a network, it is split into small pieces called packets. These packets are then transmitted over the network and reassembled at their destination. This is how data is sent between devices on the internet
- Wireless traffic can be easily captured.
  - networks like Wi-Fi or Bluetooth.
  - attackers who are within range of the wireless signal
- Some traffic is sent in plain text, making it easy to read with tools like Wireshark.
- Encrypted data can be captured but is harder to decipher.

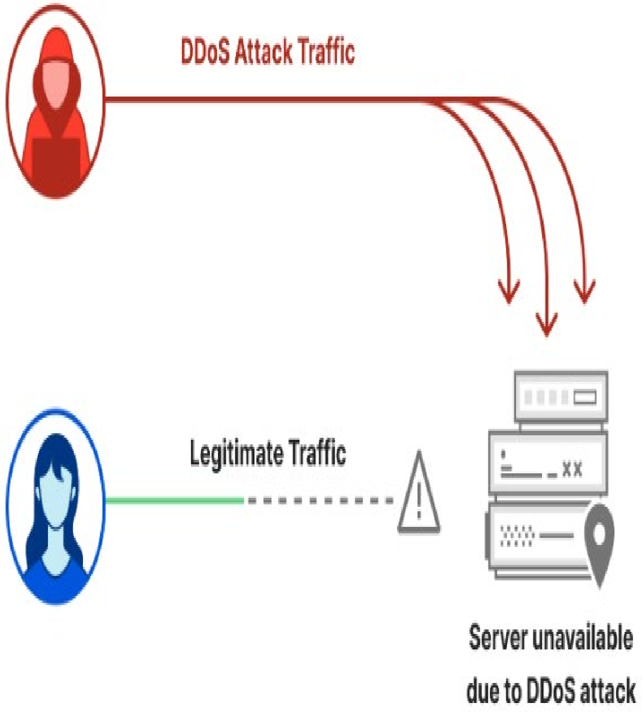
- There are several tools similar to Wireshark, which are used for network traffic analysis and packet sniffing. Some examples include:

1. Tcpdump - a command-line tool for capturing and analyzing network traffic.
2. tshark - a command-line version of Wireshark.
3. NetworkMiner - a graphical tool for network forensic analysis.
4. Ettercap - a comprehensive suite for man-in-the-middle attacks and network sniffing.
5. Ngrep - a network packet analyzer that allows users to search for specific patterns in network traffic.

- Rogue access point:
- An unauthorized access point is a rogue access point.
- They leave the network vulnerable to attacks like vulnerability scans, ARP poisoning, packet captures, and DDoS attacks.
- ARP poisoning
  - where the attacker sends fake Address Resolution Protocol (ARP) messages to a network
  - responsible for translating IP addresses into MAC addresses(unique identifiers for network devices.)

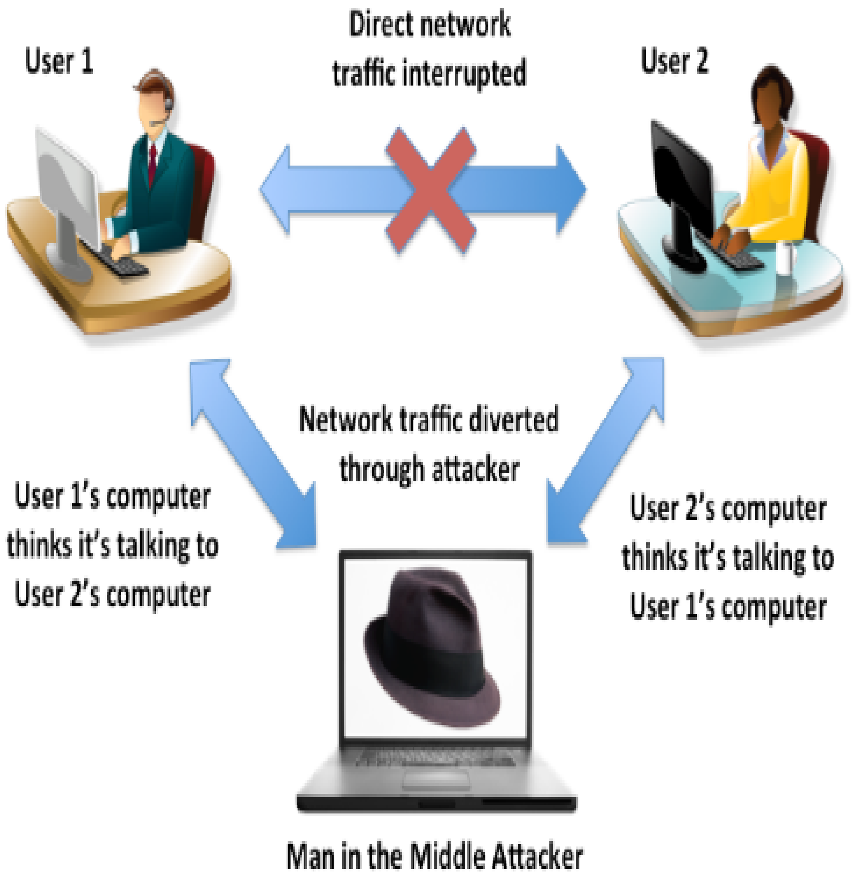
- DDoS attacks

1. A DDoS attack is a type of cyber attack that aims to overwhelm a targeted website or network with traffic.
2. Attackers use multiple systems, often controlled by botnets, to flood the target with a high volume of traffic or requests.
3. This can cause the website or network to slow down or become completely unavailable, disrupting normal business operations



- Password theft:
- Sending passwords over a network can leave them vulnerable to theft.
- Passwords sent without encryption can be read in plain text.
- Even encryption methods like SSL and TLS can be circumvented.

- Man-in-the-middle attack:
- Hackers can trick devices into sending transmissions to their system.
- They can record traffic, change file contents, insert malware, or drop communication


User 1
Direct network traffic interrupted
User 2
Network traffic diverted through attacker
User 1's computer thinks it's talking to User 2's computer
User 2's computer thinks it's talking to User 1's computer
Man in the Middle Attacker

Jamming &War driving

- Jamming floods an AP with deauthentication frames.
- This attack can overwhelm the network and prevent legitimate transmissions.
- War driving involves driving around looking for vulnerable APs to attack.
- by driving around with a wireless-enabled device and scanning for wireless network
- Attackers can use this technique to identify and exploit vulnerable networks.
- Hackers can use drones to hack APs on higher floors of buildings

- The act of driving around looking for open WI FI nodes

- There are websites and software that allows potential hackers to get a map of open APs.

- Many sites/forums with thousands of users have adopted war driving as a hobby. While many claim this to be solely as hobby, your network may be at risk if a potential hacker discovers your unsecured network

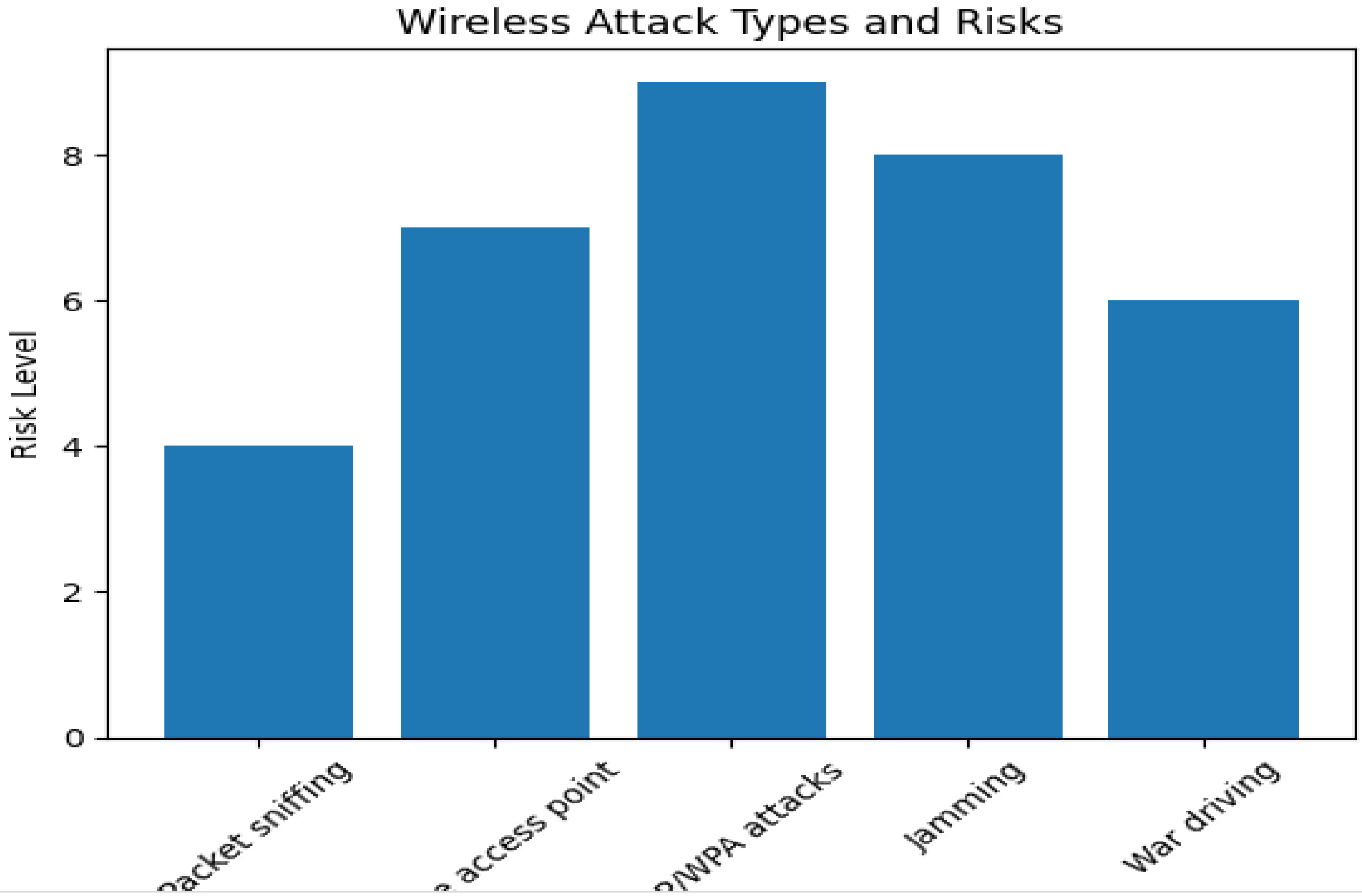
- Same sites and forums map your Wi Fi location on the internet..

- Bluetooth attacks:
- Bluetooth attacks can range from annoying pop-ups to full control over a device.

WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) are security protocols used to secure wireless networks .Attacks on wireless routers can be a significant problem.

- Older encryption standards like WEP are vulnerable.
- Once someone is on your network, you lose a layer of security.
- Public Wi-Fi networks can put your mobile devices at risk, and using a VPN can help mitigate those risks.
    - VPN hide the original IP address
    - more difficult for hackers to track your online activities

Attack type	Description	Examples	Risks	Prevention
Packet sniffing	Capturing wireless traffic in packets over a network	Wireshark	Stealing sensitive data, unauthorized access	Using encryption, using secure protocols
Rogue access point	Unauthorized access point that leaves the network vulnerable to attacks	Fake APs	Security breaches, data theft	Regularly scanning for unauthorized APs
ARP poisoning	Intercepting network traffic by modifying the ARP cache of a network	Cain and Abel	Man-in-the-middle attacks, data theft	Using ARP spoofing detection tools
DDoS attack	Flooding a targeted website or network with traffic	Botnet attacks	Disruption of services, extortion	Using DDoS protection services, having a backup server
WEP/WPA attacks	Exploiting vulnerabilities in wireless security protocols	AirSnort, Reaver	Unauthorized access, data theft	Using WPA2 with strong passwords, regular security updates
Jamming	Flooding an AP with deauthentication frames	Deauther	Network disruption, denial of service	Using APs with frequency hopping
War driving	Searching for vulnerable APs while driving around	Kismet	Unauthorized access, data theft	Regularly monitoring for rogue APs, using secure wireless protocols


Wireless Attack Types and Risks
Risk Level
0
2
4
6
8
Packet sniffing
e access point
P/WPA attacks
Jamming
War driving

Recommender Systems:

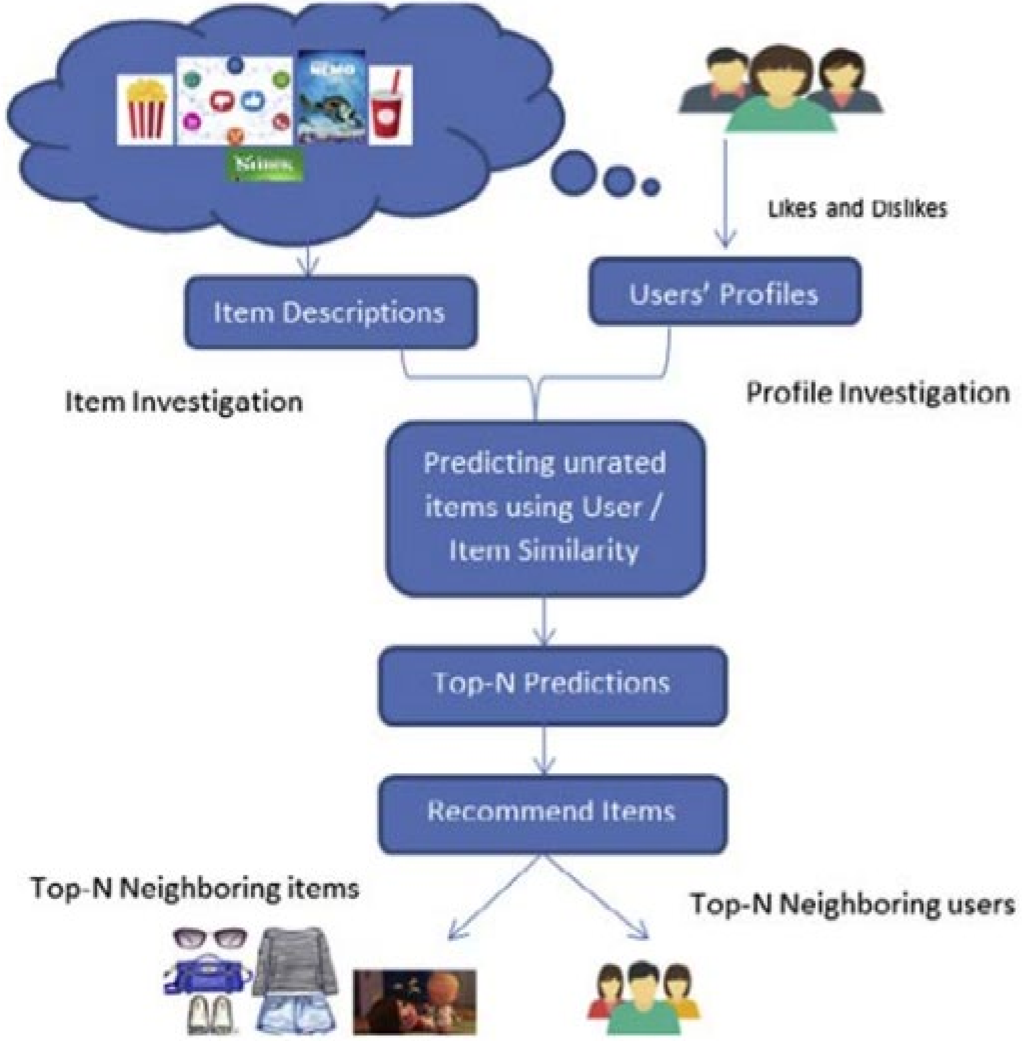
Unit IV

- We all have used services like Netflix, Amazon, and Youtube. These services use very sophisticated systems to recommend the best items to their users to make their experiences great. But, how do they achieve such great systems?

Recommender systems

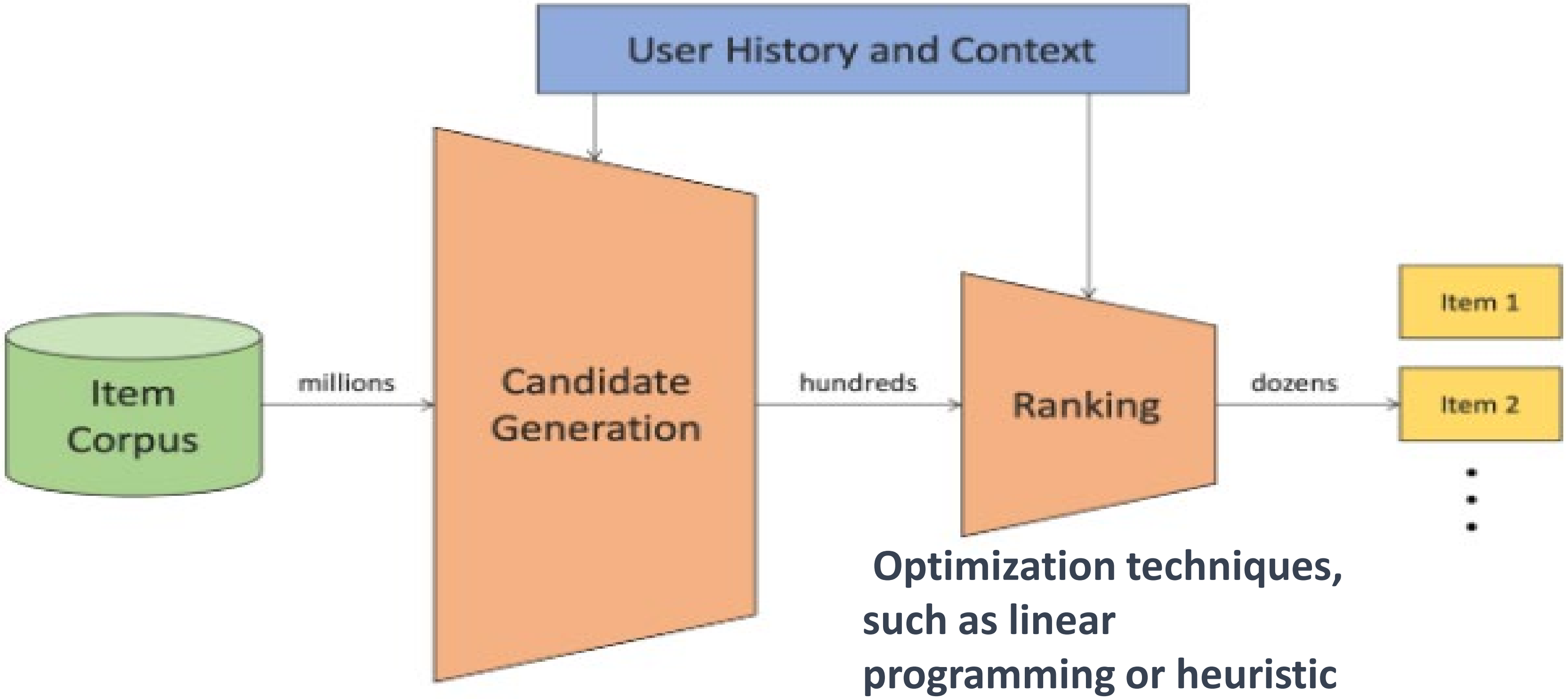
1. Recommender systems help deal with the problem of information overload by filtering and segregating information according to user preferences, interests, or observed behavior about a particular item or items.
2. Recommender systems have the ability to predict whether a particular user would prefer an item or not based on the user's profile and its historical information.
3. Recommendation systems improve decision-making processes and quality.
4. In large e-commerce settings, recommender systems enhance revenues for marketing, for the fact that they are effective means of selling more products.
5. In scientific libraries, recommender systems support and allow users to move beyond the generic catalogue searches.
6. The need to use efficient and accurate recommendation techniques within a system that provides relevant and dependable recommendations for users cannot be neglected.
7. Netflix uses a recommendation engine to present their viewers with movie and show suggestions, while Amazon uses its recommendation engine to present customers with product recommendations.
8. The general goal of both Netflix and Amazon's recommendation engines is to drive sales, boost engagement and customer retention, and deliver more personalized customer experiences.

1. Recommendations typically speed up searches and make it easier for users to access the content they have always been interested in, as well as offer them suggestions they would have never searched for.
2. Companies are able to gain new customers by sending out customized emails with links to new offers that meet the recipients' interests or suggestions of films and TV shows that suit their particular profile



Types of Recommendations

- **Editorial and hand curated**
  - List of favorites
  - Lists of “essential” items
- **Simple aggregates**
  - Top 10, Most Popular, Recent Uploads
- **Tailored to individual users**
  - Amazon, Netflix, …

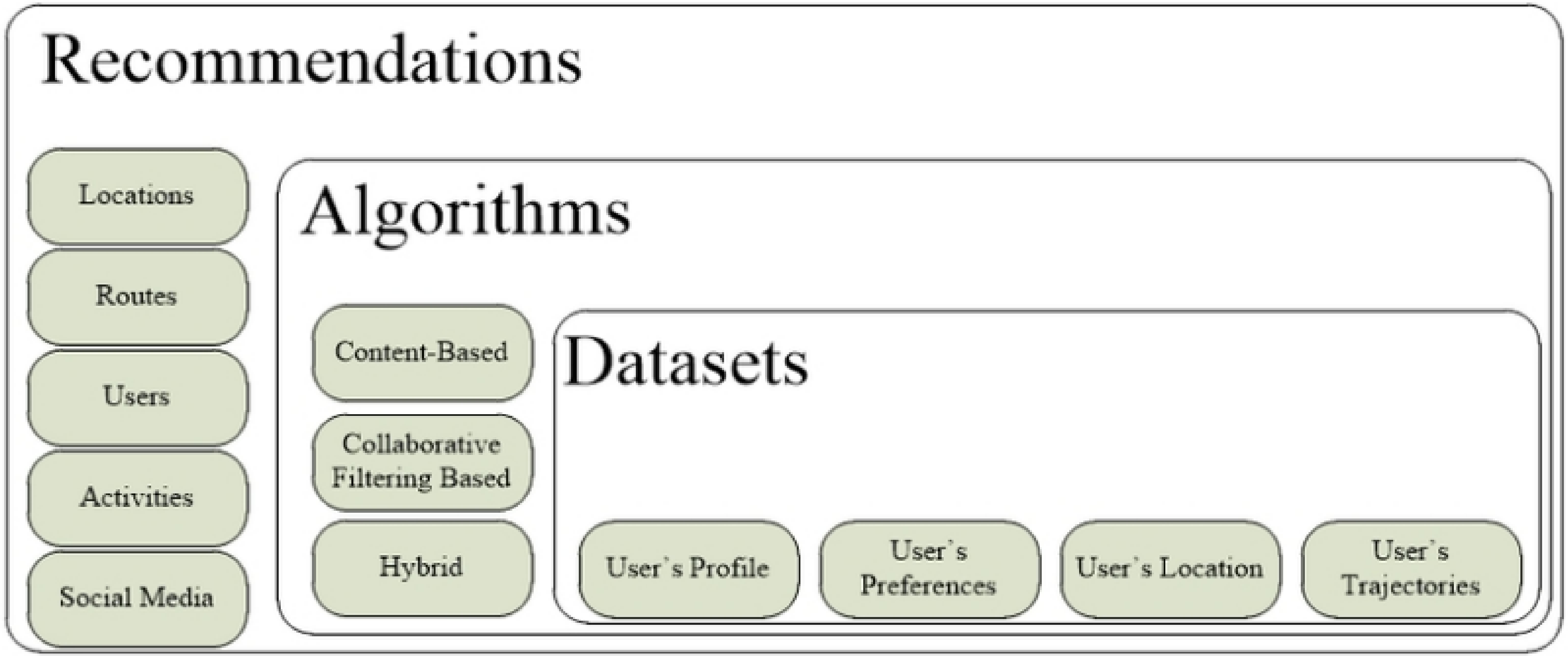


Optimization techniques, such as linear programming or heuristic algorithms.

Market basket analysis
Regression analysis
Decision trees

Recommenders mostly have 3 components

- **Candidate Generations:**
  - responsible for generating smaller subsets of candidates to recommend to a user, given a huge pool of thousands of items.
    - a subset of products based on a user's search query or browsing history.
- **Scoring Systems:**
  - Candidate Generations can be done by different Generators, so, we need to standardize everything and try to assign a score to each of the items in the subsets. This is done by the Scoring system.
    - **could assign scores to each product based on factors such as relevance, popularity, and price**
    - **feature selection, normalization, or weighting.**
- **Re-Ranking System**
  - the system takes into account other additional constraints to produce the final rankings.
  - Re-ranking systems adjust the rankings based on additional constraints.
  - Additional constraints can include user's budget, product availability, and shipping options.
  - Re-ranking systems may prioritize products that are on sale or offer free shipping based on a user's budget.
  - Re-ranking systems may exclude products that are out of stock from the final rankings


Recommendations
Locations
Routes
Users
Activities
Social Media
Algorithms
Content-Based
Collaborative Filtering Based
Hybrid
Datasets
User`s Profile
User`s Preferences
User`s Location
User`s Trajectories

Types of Candidate Generation Systems:

1. Explicit ratings: When a user explicitly rates an item, such as by giving it a star rating or a thumbs up/down, this information can be used to suggest similar items that the user might like.
2. Implicit ratings: When a user interacts with an item, such as by clicking on a link or watching a video, this behavior can be considered an implicit rating. This information can be used to suggest other items that the user might be interested in.
3. Time locality: This refers to the idea that items that a user has interacted with recently are more likely to be relevant to them than items they interacted with a long time ago. Recommender systems can take into account the temporal aspect of user behavior to suggest more relevant items.
4. Content: The content of an item, such as the words in a product description or the genre of a movie, can be used to suggest similar items. Recommender systems can use techniques such as natural language processing or image analysis to understand the content of items.
5. Sentiment: The sentiment of user reviews or comments can be used to suggest items that are more likely to be positively received by the user. Recommender systems can use sentiment analysis to understand the emotional tone of user feedback

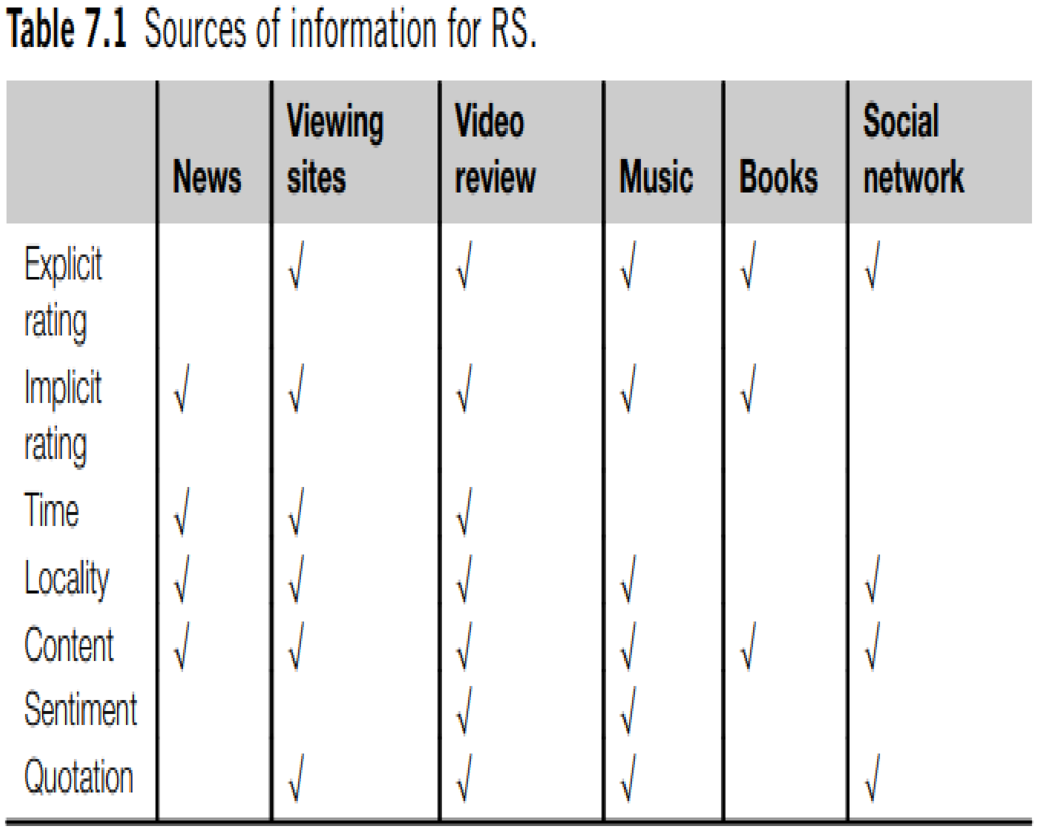
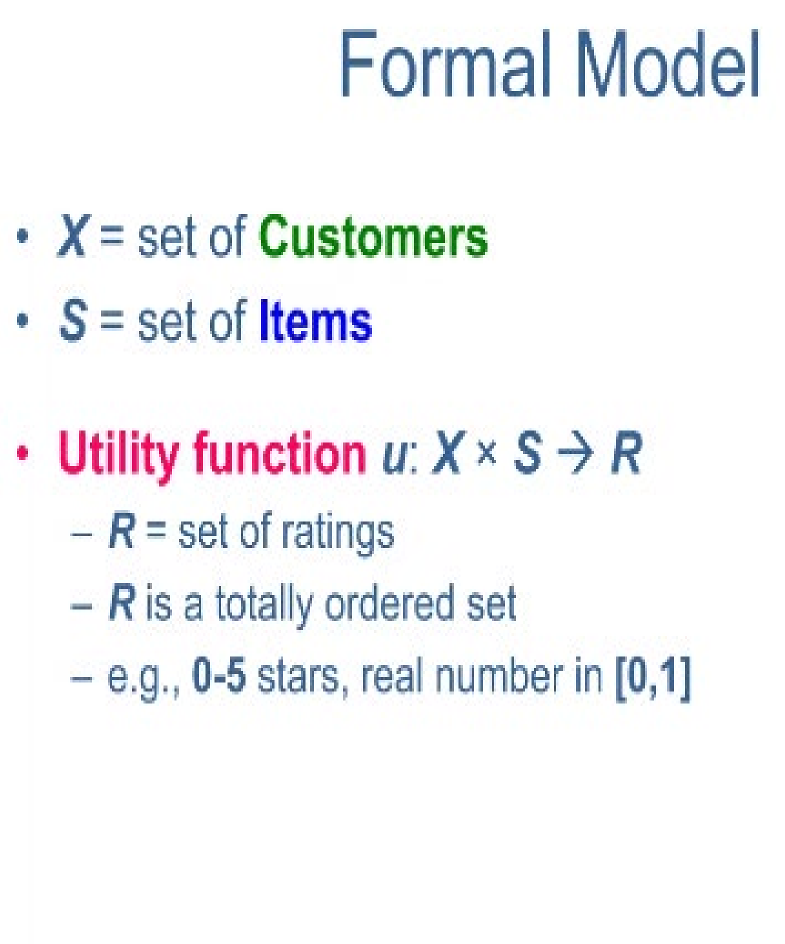


Table 7.1 Sources of information for RS.

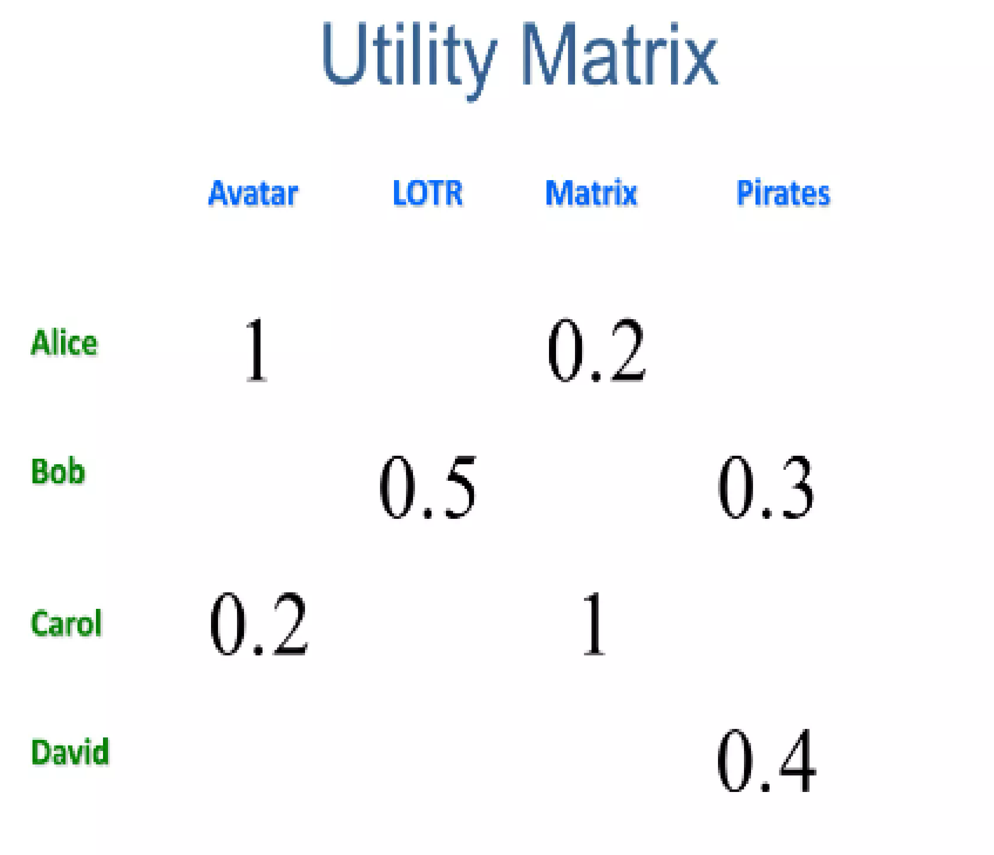
	News	Viewing sites	Video review	Music	Books	Social network
Explicit rating		√	√	√	√	√
Implicit rating	√	√	√	√	√	
Time	√	√	√			
Locality	√	√	√	√		√
Content	√	√	√	√	√	√
Sentiment			√	√		
Quotation		√	√	√		√



Formal Model

- ***X*** = set of **Customers**
- ***S*** = set of **Items**

- **Utility function *u*: *X* × *S* → *R***
  - ***R*** = set of ratings
  - ***R*** is a totally ordered set
  - e.g., **0-5** stars, real number in **[0,1]**

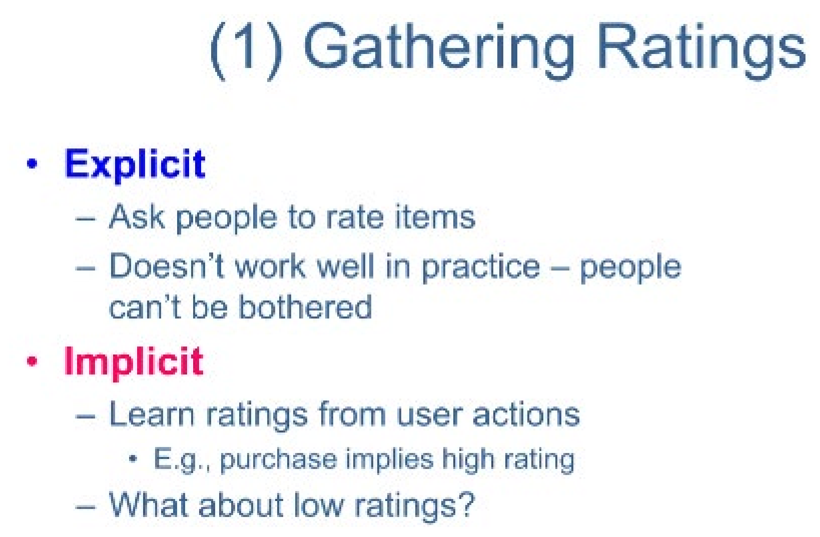


Utility Matrix

	Avatar	LOTR	Matrix	Pirates
Alice	1		0.2	
Bob		0.5		0.3
Carol	0.2		1	
David				0.4

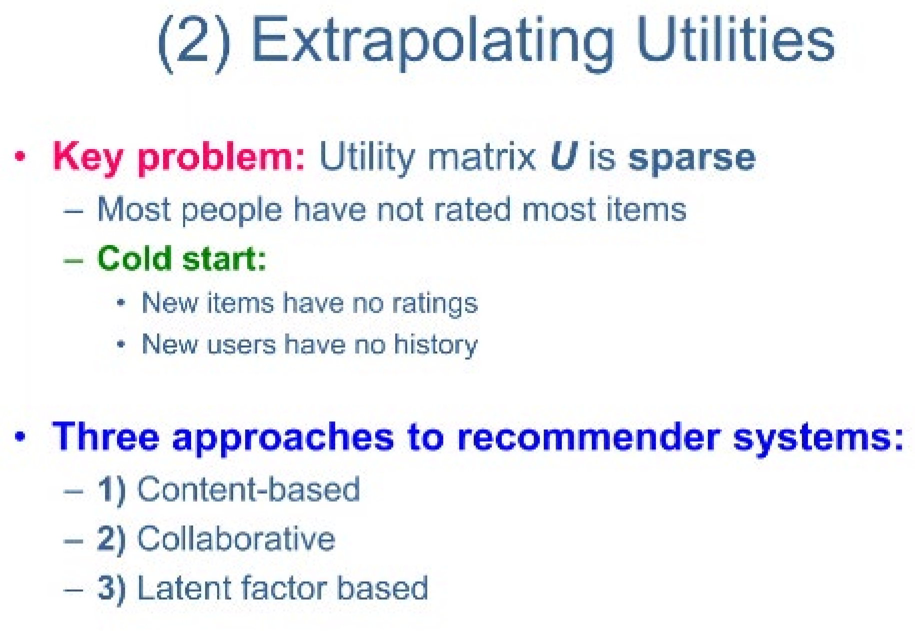
Key Problems

- (1) **Gathering "known" ratings for matrix**
  - How to collect the data in the utility matrix
- (2) **Extrapolate unknown ratings from the known ones**
  - Mainly interested in high unknown ratings
    - We are not interested in knowing what you don't like but what you like
- (3) **Evaluating extrapolation methods**
  - How to measure success/performance of recommendation methods



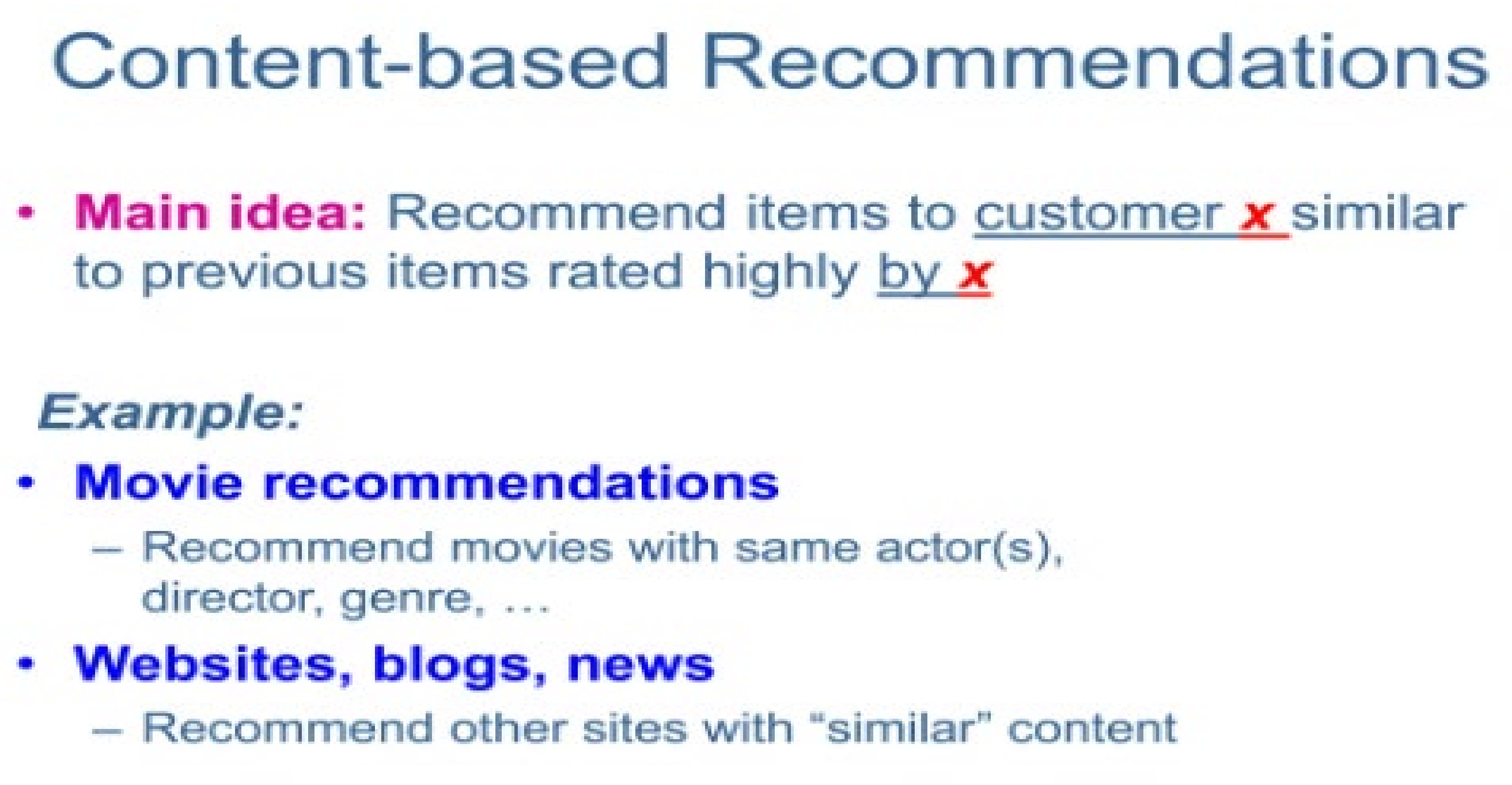
(1) Gathering Ratings

- **Explicit**
  - Ask people to rate items
  - Doesn’t work well in practice – people can’t be bothered
- **Implicit**
  - Learn ratings from user actions
    - E.g., purchase implies high rating
  - What about low ratings?



(2) Extrapolating Utilities

- **Key problem:** Utility matrix ***U*** is **sparse**
  - Most people have not rated most items
  - **Cold start:**
    - New items have no ratings
    - New users have no history
- **Three approaches to recommender systems:**
  - **1)** Content-based
  - **2)** Collaborative
  - **3)** Latent factor based



Content-based Recommendations

- **Main idea:** Recommend items to customer *x* similar to previous items rated highly by *x*

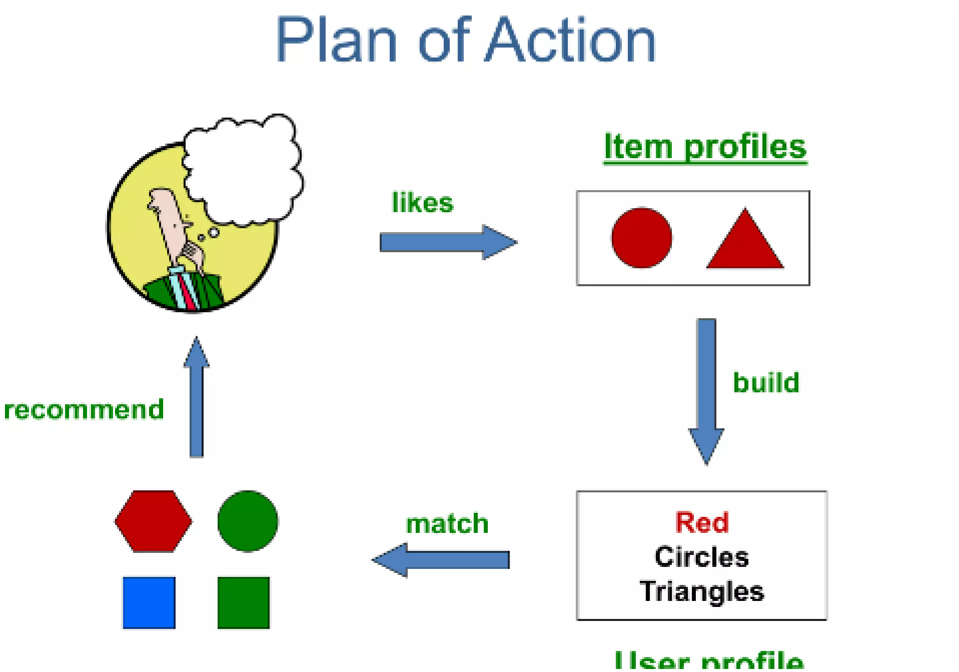
Example:

- **Movie recommendations**
  – Recommend movies with same actor(s), director, genre, …
- **Websites, blogs, news**
  – Recommend other sites with "similar" content

The content or attributes of the things you like are referred to as "content."

USES PAST USER-ITEM INTERACTIONS TO PRODUCE NEW RECOMMENDATIONS

1.Content-based recommendation systems aim to match users with items based on the items' content, such as genre, color, etc.
2.These systems also utilize users' profiles, including their likes, dislikes, and demographic information, to suggest items that are more likely to be of interest to them.
3.An example of content-based recommendation is YouTube suggesting cooking videos to a chef who has watched a lot of baking videos in the past.
4.Content-based recommendation systems are effective for recommending items that have clear and distinct features or attributes, such as music or movies



Plan of Action

Item profiles

likes

build

Red
Circles
Triangles

User profile

match

recommend

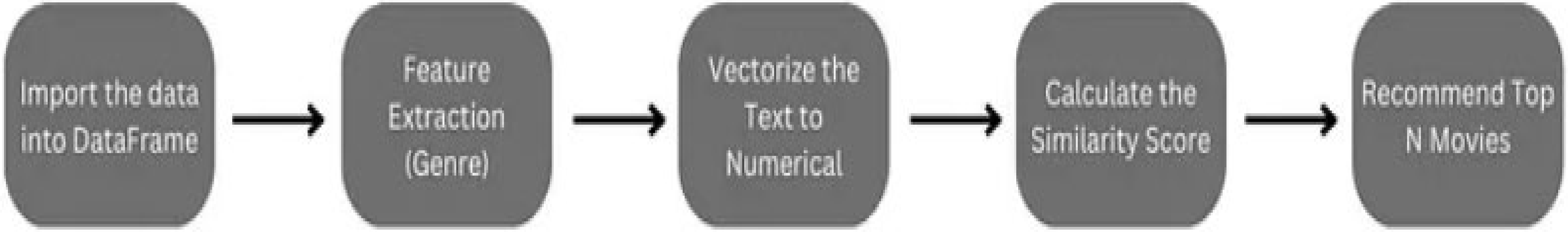
Item Profiles

- For each item, create an **item profile**
- **Profile is a set (vector) of features**
  - **Movies:** author, title, actor, director,…
  - **Text:** Set of "important" words in document
- **How to pick important features?**
  - Usual heuristic from text mining is **TF-IDF** (Term frequency * Inverse Doc Frequency)
    - Term … Feature
    - Document … Item

1. Pearson Correlation Coefficient: It measures the linear correlation between two variables and is commonly used in recommendation systems.
2. Cosine Similarity: It measures the cosine of the angle between two vectors and is widely used in recommendation systems due to its ability to handle sparse data.
3. Jaccard Similarity: It measures the similarity between two sets and is often used in recommendation systems for binary data.
4. Euclidean Distance: It measures the straight-line distance between two points in a multi-dimensional space and is often used in recommendation systems.
5. Manhattan Distance: It measures the absolute differences between two points in a multi-dimensional space and is often used in recommendation systems.

- **Cosine similarity is often considered the best measure for content-based recommendation systems as it is well suited for sparse data**

Steps Involved:

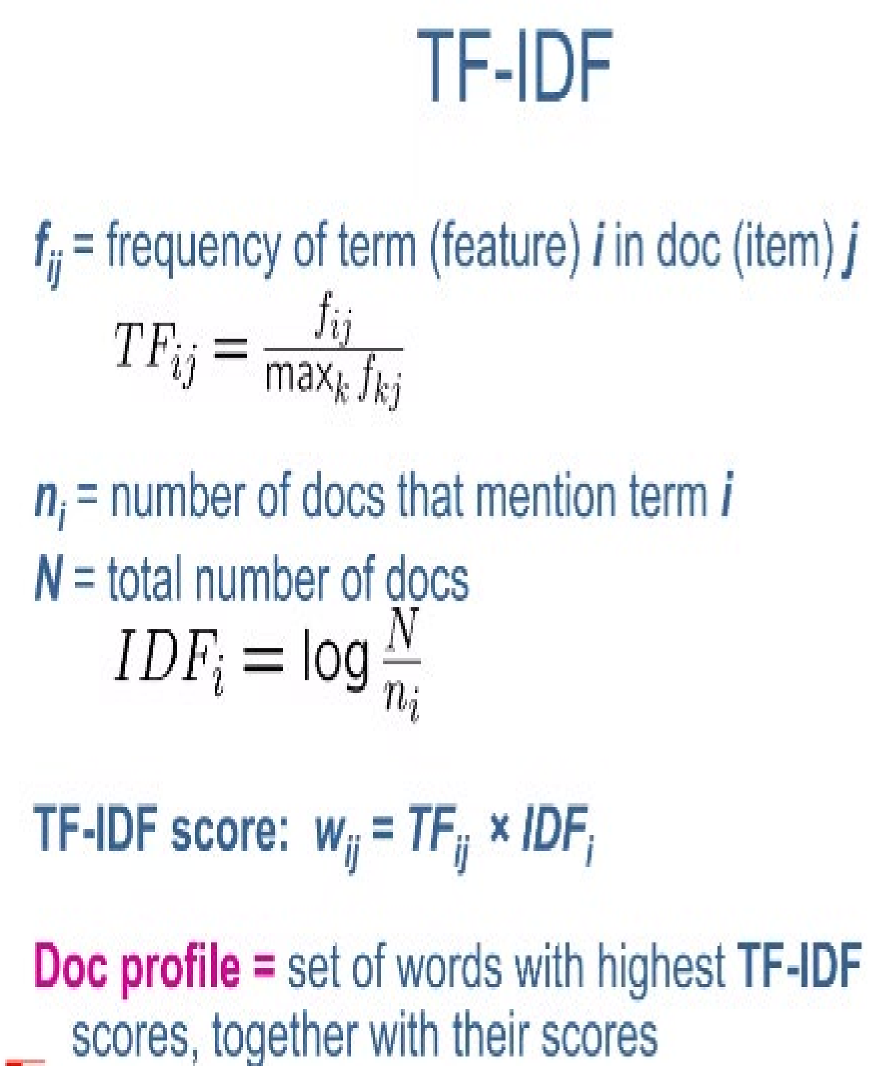


Import the data into DataFrame → Feature Extraction (Genre) → Vectorize the Text to Numerical → Calculate the Similarity Score → Recommend Top N Movies

To build a basic movie recommendation system by just using genre column as feature

- **3 DIFFERENT VECTORIZERS**:

1. Binary Feature Matrix
2. Bags of Words
3. Tf-IDF



TF-IDF

f_{ij} = frequency of term (feature) i in doc (item) j

$$TF_{ij} = \frac{f_{ij}}{\max_k f_{kj}}$$

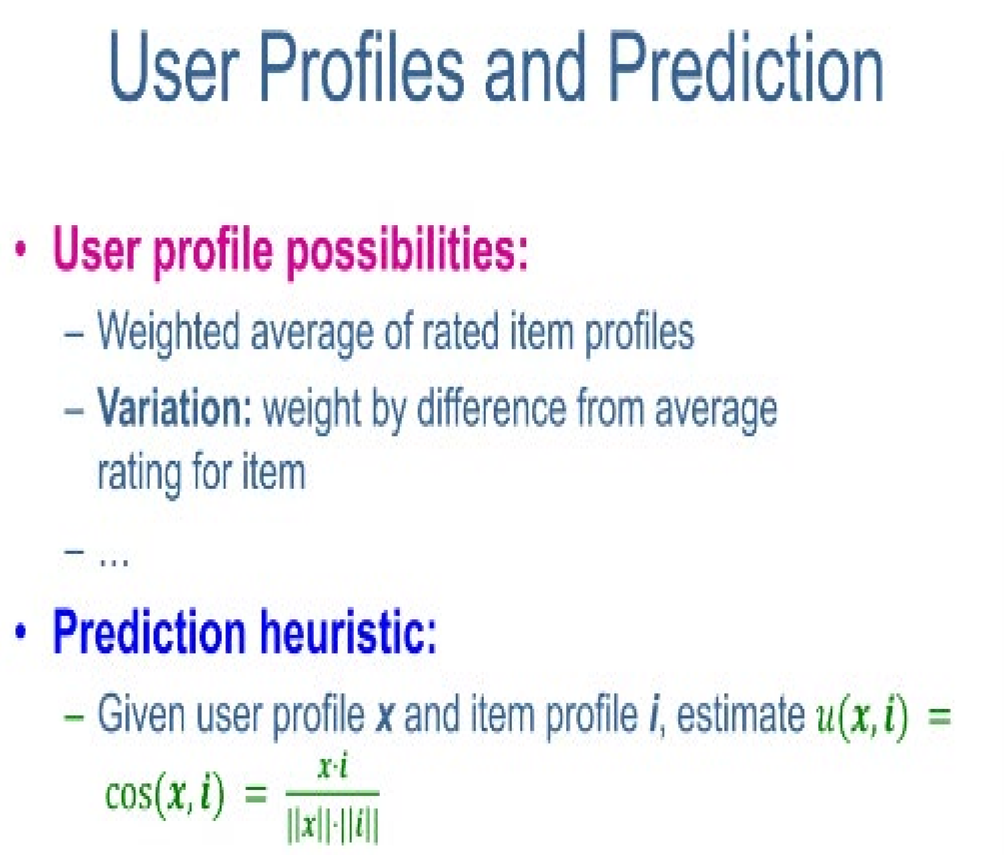
n_i = number of docs that mention term i

N = total number of docs

$$IDF_i = \log \frac{N}{n_i}$$

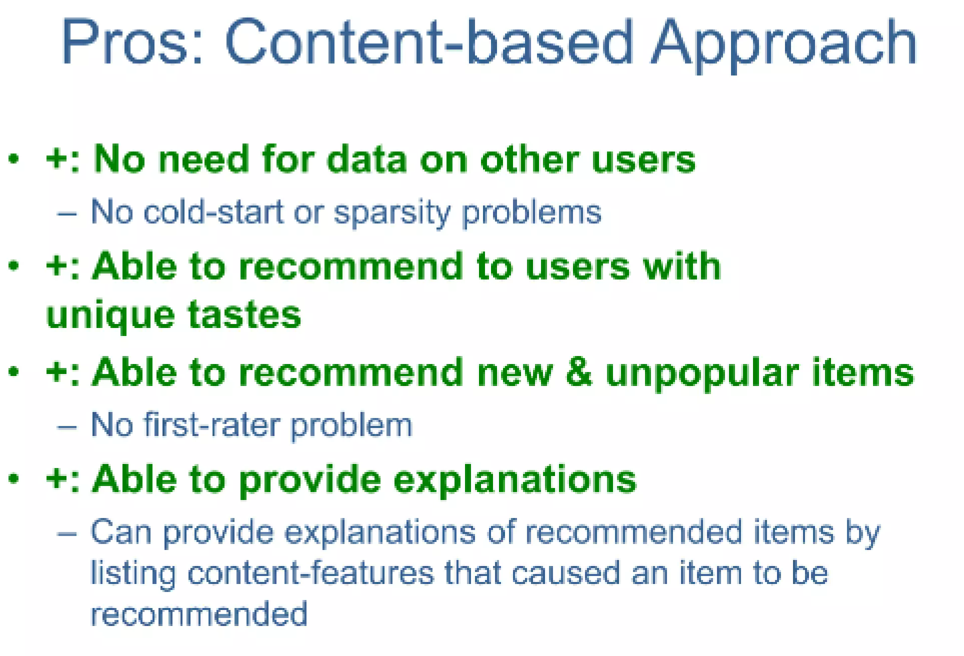
TF-IDF score: $w_{ij} = TF_{ij} \times IDF_i$

Doc profile = set of words with highest **TF-IDF** scores, together with their scores



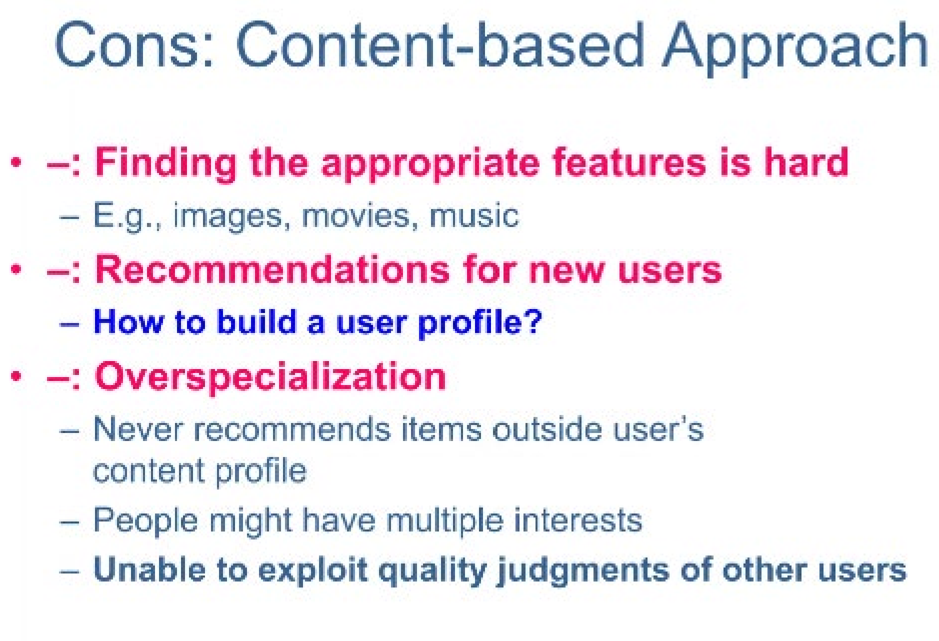
User Profiles and Prediction

- **User profile possibilities:**
  - Weighted average of rated item profiles
  - **Variation:** weight by difference from average rating for item
  - …
- **Prediction heuristic:**
  - Given user profile $\boldsymbol{x}$ and item profile $\boldsymbol{i}$, estimate $u(\boldsymbol{x}, \boldsymbol{i}) = \cos(\boldsymbol{x}, \boldsymbol{i}) = \frac{\boldsymbol{x} \cdot \boldsymbol{i}}{||\boldsymbol{x}|| \cdot ||\boldsymbol{i}||}$



Pros: Content-based Approach

- **+: No need for data on other users**
  - No cold-start or sparsity problems
- **+: Able to recommend to users with unique tastes**
- **+: Able to recommend new & unpopular items**
  - No first-rater problem
- **+: Able to provide explanations**
  - Can provide explanations of recommended items by listing content-features that caused an item to be recommended



Cons: Content-based Approach

- **–: Finding the appropriate features is hard**
  - E.g., images, movies, music
- **–: Recommendations for new users**
  - **How to build a user profile?**
- **–: Overspecialization**
  - Never recommends items outside user's content profile
  - People might have multiple interests
  - **Unable to exploit quality judgments of other users**

- Imagine you are building a movie recommendation system for a streaming platform. What factors would you consider when selecting movies to recommend to a user?
    - When building a movie recommendation system, we would consider various factors such as user preferences, viewing history, genre, ratings, popularity, and release date. We could also incorporate external data sources such as movie reviews, critic ratings, and social media buzz to improve the recommendations.

Suppose you are building a product recommendation system for an e-commerce website. How would you deal with the cold start problem for new users who have not provided any data on their preferences?

- ❑The cold-start problem is generating personalized recommendations for new users/items without any data.
- ❑To address the cold-start problem for new users, content-based and knowledge-based recommendations can be used.
- ❑To address the cold-start problem for new items, popularity-based and hybrid recommendations can be used

- You are building a music recommendation system for a music streaming app. How would you incorporate the temporal dynamics of music preferences into your recommendation algorithm?

- When incorporating the temporal dynamics of music preferences into our recommendation algorithm, we could use techniques such as matrix factorization, which can capture the changes in users' preferences over time. We could also use session-based recommendations that suggest music based on the user's current listening session and context.

- Suppose you are building a news article recommendation system for a news website. How would you ensure that the recommended articles are diverse and cover a wide range of topics?

- To ensure that the recommended articles are diverse and cover a wide range of topics, we could use techniques such as topic modeling, which can identify the underlying themes and topics of the articles. We could also use diversity-aware recommendation algorithms that promote variety and novelty in the recommendations.

- You are building a food recommendation system for a restaurant review website. How would you incorporate user preferences and dietary restrictions into your recommendation algorithm?

- To incorporate user preferences and dietary restrictions into our recommendation algorithm for a food recommendation system, we could use content-based recommendations that consider the ingredients and nutritional information of the dishes. We could also use hybrid recommendations that combine content-based and collaborative filtering techniques to generate more personalized recommendations

- Suppose you are building a travel recommendation system for a travel booking website. How would you incorporate user feedback and ratings into your recommendation algorithm?

- To incorporate user feedback and ratings into our travel recommendation algorithm, we could use collaborative filtering techniques that rely on similar users' preferences to generate recommendations. We could also use sentiment analysis and natural language processing techniques to analyze the user's feedback and extract useful insights

- You are building a social media recommendation system for a social networking app. How would you incorporate the social network structure and user interactions into your recommendation algorithm

When building a social media recommendation system, we could incorporate the social network structure and user interactions by using graph-based recommendation algorithms that consider the network topology and the strength of the connections between users. We could also use content-based recommendations that consider the user's interests, preferences, and past interactions.

- To incorporate user skill level and game genre preferences into our video game recommendation algorithm, we could use collaborative filtering techniques that rely on similar users' preferences to generate recommendations. We could also use content-based recommendations that consider the game's attributes and features, such as difficulty level, genre, and gameplay mechanics.

Quality metrics for recommender systems along with their formulas:

Metric	**Formula**
Accuracy	(Number of correct recommendations) / (Total number of recommendations)
Precision	(Number of relevant recommended items) / (Total number of recommended items)
Recall	(Number of relevant recommended items) / (Total number of relevant items in the system)
Coverage	(Number of recommended items) / (Total number of items in the system)
Diversity	1 - (Average similarity between recommended items)
Novelty	(Average novelty of recommended items)
Serendipity	(Average serendipity of recommended items)

- Suppose you have a movie recommendation system that recommends movies to users based on their past viewing history and ratings. Let's say the system recommends five movies to a user, and we want to evaluate the quality of these recommendations using some of the metrics we discussed earlier.
- Accuracy: Let's say the user has seen four of the five recommended movies before, and only one is a new recommendation. Then the accuracy of the system would be:
- **Accuracy = (4 correct recommendations) / (5 total recommendations) = 0.8 or 80%**
- Precision and Recall: Let's say two of the recommended movies are relevant to the user's interests, and three are not. Then the precision of the system would be:
- Precision = (2 relevant recommended items) / (5 total recommended items) = 0.4 or 40%
- The recall of the system would be:
- Recall = (2 relevant recommended items) / (Total number of relevant items in the system) = (2 relevant recommended items) / (Total number of movies user likes)
- Coverage: Let's say the system has a total of 10,000 movies in its inventory, and it recommended 50 movies to the user in the past month. Then the coverage of the system would be:
- Coverage = (50 recommended items) / (10,000 total items in the system) = 0.005 or 0.5%
- Diversity: Let's say the recommended movies are all from the same genre, and there are no recommendations from other genres. Then the diversity of the system would be low.
-

Aspect	Collaborative Filtering (CF)	Content-Based Filtering (CBF)
Definition	Recommends items based on the similarity between users' preferences	Recommends items based on their attributes or features
Data Requirements	User preferences and item ratings	Item attributes or features
Types of Recommendations	Recommends items liked by similar users but not seen by the user	Recommends items similar to ones the user has liked before
User Independence	Dependent on having a community of users to provide feedback	Independent of user feedback
Cold Start Problem	Suffers from the cold start problem for new users	Does not suffer from the cold start problem
Diversity of Recommendations	Tends to recommend popular items resulting in less diverse recommendations	Can provide more diverse recommendations
Domain Applicability	Effective for domains with frequently	Suitable for domains with stable

Forensic Analysis

- Aim :
- Examine the relevance and usability of digital investigation to explore the evidence of digital crimes.
- Observe the facilities of digital forensics to understand the behavioral and emotional analysis.
- social behavioral analysis (SBA) :inductive
- subset of behavioral evidence analysis (S-BEA) : a forensic tool used to analyze the behavior of offenders in criminal investigations

- Social media content is frequently examined in criminal investigations, particularly in cases involving personal or financial issues.
- Legal practitioners and law enforcement organisations are both involved in gathering important information in order to analyse suspicious evidence.
- Because of the complexity and amount of forensic information, automated techniques must be used to efficiently handle duties and obtain technological evidence.

- Not ideal for digital forensics due to legal limitations of data provenance and inability to trace data origin
    - Data mining approaches using natural language processing
    - Study Reveals Link Between Social Media Use and Depression
- The evolution of the internet
    - created opportunities for criminality and mismanagement.
    - Connected environments make it easier for illegal behavior to occur.
- Anonymity in online environment
    - to reduce the risk of contact and facilitate illegal activities.
- Criminals can use social networks and online tools to prepare for illegal activities and target naive users.
- Criminals can use online profiles to scam people for monetary gain

- Cyber stalking is a type of online crime.
  - It involves repeated use of electronic communication to harass, intimidate or threaten someone.
  - Cyber stalkers use various tactics to monitor their victim's online activity.
  - These tactics include hacking into their email or social media accounts, creating fake profiles, and using GPS tracking to monitor their movements.
- Cyber vandalism
  - act of intentionally damaging or destroying computer systems, networks, websites, or other digital assets.
  - hacking into a website and defacing its content
  - planting viruses or malware
  - disrupting the normal functioning of computer systems
  - stealing sensitive data.

Investigation models in digital forensic

- Digital evidence needs to be regulated and standardized to ensure accuracy and admissibility in court.
- Inconsistencies in models and regulations can lead to imperfect evidence and inaccurate interpretation.
- A standard forensic model can improve technical accuracy and facilitate digital applicability and research direction.
- Technical experts are developing a standard evidence model to critique and improve digital forensics.

Model 1: crime scene investigation

- **Secure and Scene Evaluation**
  - Identify and secure the location of the crime scene
  - Protect potential evidence from tampering or destruction
  - Ensure the safety of investigators and any individuals present at the scen
- **Criminal Documentation**
  - Document the crime scene and any potential evidence
  - Establish a clear chain of custody for the evidence
  - Provide a record of the evidence collected
- **Collecting the Evidence**
  - Identify potential electronic evidence, such as computer hard drives, mobile devices, or other digital storage media
  - Use specialized tools and techniques to collect the evidence in a manner that is legally admissible and preserves the integrity of the evidence
  - Record the location, time, and individuals involved in the evidence collection process
- Transporting the Digital Evidence
  - Transport the collected evidence to a secure location, such as a crime lab
  - Handle the evidence carefully to avoid damage or tampering
  - Maintain a clear chain of custody documentation to ensure the integrity of the evidence is preserved

Model 2: abstract digital forensics

1. Digital identification: The investigators start by identifying the social media platform and the specific account used for cyberbullying. They also gather any other relevant digital identifiers, such as IP addresses or device IDs associated with the account.
2. Evidence preparation: The investigators collect and preserve any evidence related to the cyberbullying, such as screenshots of offending posts or messages.
3. Strategy development: The investigators develop a strategy for collecting additional evidence, such as identifying the location of the perpetrator or any other accounts they may be using.
4. Evidence collection: The investigators use various methods to collect additional evidence, such as social engineering or data mining tools, to identify other accounts linked to the perpetrator.
5. Modeling examination: The investigators create a model of the perpetrator's online behavior and examine it to identify patterns or anomalies that may help identify the individual.
6. Data analysis: The investigators analyze the evidence collected to determine the perpetrator's identity, location, or other relevant information.
7. Evidence presentation: The investigators present their findings and evidence in court, using the digital evidence collected to support their case.
8. Belief reinforcement: The investigators continue to monitor the perpetrator's online activity to reinforce their belief in the accuracy and reliability of their evidence.

Model 3:Integrated investigation process

1. Promptness: The investigation process should begin as soon as possible after the crime is reported to minimize the loss or tampering of physical or digital evidence.
2. Placement: This group involves identifying the location of the physical and digital crime scenes and coordinating the efforts of forensic investigators to collect evidence from both.
3. Physical crime scene: The physical crime scene group is responsible for collecting and analyzing physical evidence, such as fingerprints or DNA samples.
4. Digital crime scene: The digital crime scene group is responsible for collecting and analyzing digital evidence, such as social media posts or computer files.
5. Investigation review: This group involves reviewing and analyzing all of the evidence collected during the investigation and using it to identify potential suspects and build a case.

Model	Description
Model 1	A criminal investigation model that includes documenting the crime scene, identifying potential evidence, collecting and transporting digital evidence, storing data, analyzing evidence, and concluding the investigation.
Model 2	An abstract digital forensic model that includes digital identification, evidence preparation, strategy development, evidence collection, examination, data analysis, digital evidence presentation, and belief return.
Model 3	An integrated investigation model that combines physical and digital crime investigation and includes promptness, placement, physical crime scene, digital crime scene, and investigation review.
Model 4	A hierarchical objective-based (HOB) framework that investigates digital evidence through six phases, including preparing digital evidence, creating incident response, collecting digital data, analyzing evidence, presenting digital findings, and returning incidental closure.
Model 5	Cohen's digital forensics model that addresses legal issues and represents forensic elements such as investigation, clarification, ascription, and reconstruction.
Model 6	A systematic forensic investigation model that includes organized preparation, securing criminal scenes, recognizing review materials, documenting crime scenes, communicating evidence, collecting criminal data, preserving the crime scene, examining criminal data, analyzing the crime, presenting criminal defense, and presenting crime scene results.

Model	**Key Components**
7model 7	- Detecting the incidental request - Planning the investigation - Preparing the criminal scene - Identifying potential evidence - Collecting, transporting, and storing digital evidence - Analyzing the evidence - Concluding the investigation
Model 8	- Promptness in responding to the incident - Identifying the crime scene - Collecting the crime scene - Examining digital evidence - Analyzing the crime scene - Presenting the digital evidence - Concluding the investigation

Model	Key Components
9	- Acquiring digital evidence - Examining digital information - Planning the investigation - Identifying evidence - Collecting digital data - Storing and transporting information - Analyzing digital grounds - Creating proofs - Archiving evidence - Presenting evidence
10	- Previous models focus on high-level investigation - Additional specific steps include constituting the evidence and identifying guidelines - Limited specificity and adaptability to different types of digital crimes and forensic scenarios - Lack of standardization and consistency in the terminology and procedures used in different investigations

Integrating behavioral analysis:Cyberstalker: forensic methodology

1. The methodology developed by Slide et al. combines behavioral analysis and standard forensic investigation techniques to investigate cyberstalking cases.
2. The methodology involves three main steps: discovering the digital evidence, examining the digital data, and analyzing the evidence.
3. The methodology includes an evaluation method that assesses the utility of the model to simulate a predefined set of cyber activities.
4. The researchers also examine the victim's evidence and the criminal technologies used in the cyberstalking activities.
5. The methodology helps investigators understand the stalker's behavior patterns and motivations, which can be useful in identifying the suspect and building a case against them.
6. The article emphasizes the importance of interdisciplinary collaboration between forensic investigators, law enforcement agencies, and mental health professionals in addressing cyberstalking cases

Roger's behavioral analysis is a model

- digital forensics investigation
  - engineering principles involved in the investigation process
    - case classification- scams, cyberstalking, or data theft
    - contextual analysis- understanding the digital circumstances to deliver the relevant evidence
    - digital data collection- the investigator works with interactive analysts to search for relevant data to prepare the digital evidence
    - visualization of digital evidence-such as timelines, network graphs, heat maps, and 3D visualizations
    - and conclusion/opinion-investigators to identify patterns, relationships, and anomalies in the data, which can provide valuable insights for the investigation.

Attacks based on communication

Recap

- Introduction to smartphone security threats
    - malware, phishing attacks, insecure Wi-Fi networks,
- Overview of security measures
    - to protect users, such as encryption, biometric authentication, two-factor authentication, etc.
- User awareness
    - common mistakes that users make, such as using weak passwords, downloading apps from untrusted sources, clicking on suspicious links, etc.
- Future trends
    - the use of artificial intelligence
        - to detect and prevent security threats
    - the adoption of blockchain technology

Attacks based on communication

- Smartphone users face various threats that can harm their device and their data.
- Applications must ensure the privacy and security of the user's information.
- Some apps may be malware, so their activities must be limited.
- Restrictions can be placed on apps, such as blocking access to the user's location or address book, preventing data transmission on the network, and limiting SMS messaging.

Smartphones are prime targets for attackers: Three Prime Targets For Attackers Are Data, Identity, And Availability.

- **Data:** A user may have their credit card information stored in a mobile payment app on their smartphone. An attacker could try to gain access to this information through a phishing scam or by exploiting a vulnerability in the app's security.
- **Identity:** A user's smartphone can contain a lot of personal information, including their name, address, and phone number. An attacker could use this information to impersonate the user or to commit identity theft.
- **Availability**: An attacker could use a denial-of-service (DoS) attack to prevent a user from accessing their smartphone. For example, the attacker could flood the user's smartphone with requests, overwhelming the device and rendering it unusable. Alternatively, an attacker could install malware on the device that causes it to crash or freeze, making it difficult for the user to use their smartphone.

Various threats to mobile devices

- Annoyance
  - Adware is a type of annoyance
    - bombards the user with unwanted advertisements
    - an app display pop-up ads or redirect the user to unwanted website
- stealing money
  - banking Trojans can steal sensitive information
- Invading privacy
  - spyware can be used to monitor a user's activity and steal personal information
    - nefarious purposes, such as identity theft or blackmail
- Propagation
  - Malware can spread quickly and easily from device to device
    - user could receive an email that appears to be from a trusted source
      - phishing email that installs malware on the device
- Malicious tools
  - remote access tool
    - gain control of a user's device and steal sensitive information,
  - use ransomware
    - to lock the device and demand payment in exchange for access.

Common Tactics Used By Cybercriminals

- Botnets
  - carry out distributed denial of service (DDoS) attacks or to send spam email
  - Botnets are used to infect multiple machines with malware.
- Victims can acquire malware through email attachments or compromised applications/websites.
- Malware gives hackers remote control of "zombie" devices to perform harmful acts.
  - the hacker can use that device to perform harmful acts without the user's knowledge or consent
- Malicious applications can steal personal information and install additional harmful applications.
- Malicious links on social networks can spread Trojans, spyware, and backdoors.
- Spyware allows hackers to hijack phones and monitor calls, texts, emails, and location.
- Users should stay vigilant and protect their devices and personal information

Sources Of Mobile Attacks

	Black Hat Hackers	Gray Hat Hackers
Motivation	Personal gain	Security testing and research
Goal	Cause damage, steal data	Expose vulnerabilities and help to address them
Ethics	Unethical	Ethical, but not always legal
Method	Use malicious techniques to exploit vulnerabilities	Use non-destructive techniques to identify vulnerabilities
Examples	Spreading malware, stealing data for personal gain	Revealing vulnerabilities to the public, helping to improve security

Smartphone Is Infected By An Attacker

- An attacker can use a compromised smartphone as a zombie machine to send spam messages via SMS or email.
- The attacker can force the smartphone to make phone calls, which can result in charges to the owner or disruption of emergency services.
- A compromised smartphone can record conversations between the user and others and send them to a third party, compromising privacy and security.
- An attacker can steal a user's identity by copying their SIM card or phone, and impersonate the owner, which raises security concerns in countries where smartphones are used as identity cards or for financial transactions.
- The attacker can drain the smartphone's battery by running energy-intensive applications, causing it to become less useful.
- The attacker can prevent the smartphone from functioning by deleting boot scripts, modifying files, or embedding a startup application that would empty the battery.
- The attacker can also remove personal or professional data from the smartphone, such as photos, music, contacts, calendars, and notes

Attack based on SMS and MMS

- Some attacks on mobile phones are caused by flaws in the management of SMS and MMS messages.
- Some mobile phone models have problems handling binary SMS messages, which can cause the phone to restart and lead to DDoS attacks.
- Certain Nokia phones didn't verify the standard for email address size, so entering an email over 32 characters could disable the email handler.
- SMS messages sent from the internet can be used to perform DDoS attacks against a mobile telecommunications network.
- An MMS message with an infected attachment can infect a user's phone and send infected messages to all their contacts. The virus Commwarrior is an example of this type of attack

Portability of malware across platforms

1. Malware can target multiple platforms and can be spread to different systems
2. Malware can use runtime environments like Java virtual machine or the .NET Framework and other libraries present in many operating systems.
3. Memory cards and synchronization software can be used for this purpose, or to propagate the virus.
4. Resource monitoring in the smartphone can detect the activity of a malicious application.
5. Battery and memory usage can be monitored to detect certain malware applications.
6. Network traffic, services, and network surveillance can also be monitored to detect suspicious activity.
7. Spam filters and encryption of stored or transmitted information can minimize spam campaigns and prevent data interception.
8. Telecom network monitoring can quickly detect potential threats.
9. Manufacturers should remove debug mode and ensure correct default settings in smartphones