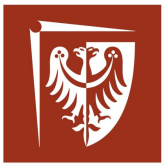


Politechnika
Wrocławska

Politechnika Wrocławska
Wydział Elektroniki

Obrona Magisterska 2020

Kierunek:
Informatyka techniczna(INF)
Specjalizacja:
Grafika i systemy multimedialne(IGM)

21 września 2020

Spis treści

1 Pytania Kierunkowe

1.1 Metody uwierzytelniania użytkowników w systemach komputerowych - sposoby, wady, zalety

W systemach komputerowych wykorzystywane są dwa podstawowe elementy identyfikacji użytkowników, które ze względu na podobieństwo nazw, są często mylone:

- **Autentykacja** (ang. *authentication*) - Często nazywana uwierzytelnieniem, określa, czy użytkownik jest tym, za kogo faktycznie się podaje, przy wykorzystaniu odpowiedniego rodzaju poświadczeń tożsamości.
- **Autoryzacja** (ang. *authorization*) - Definiuje do jakich zasobów bądź operacji użytkownik o danej tożsamości ma dostęp.

Pytanie odnosi się bezpośrednio do pojęcia autentykacji, warto więc pamiętać, że w jego zakres nie wchodzą zagadnienia dotyczące drugiej z metod. Ze względu na wykorzystywane do autentykacji informacje, można podzielić sposoby identyfikacji użytkownika na trzy główne grupy:

- **Coś co wiesz** - Informacje których świadomy jest użytkownik systemu, przykładowo:
  - Login i hasło,
  - Unikatowy klucz dostępu do systemu,
  - Dane tożsamościowe, np. PESEL, numer dowodu osobistego
- **Coś co masz** - Informacje dostarczane przez urządzenia, które użytkownik posiada, przykładowo:
  - Kod weryfikacyjny z SMS lub autentykatora TOTP (Google Authenticator, Authy, itp.). Kody takie są zazwyczaj jednorazowe, oraz posiadają krótki okres ważności (w przypadku TOTP, jest to 30s),
  - Klucz fizyczny, często podłączany do portów USB (YubiKey) lub w formie karty wkładanej do czytnika (SmartCard), zawierający unikatowy dla użytkownika token umożliwiający autentykację.
- **Coś czym jesteś** - Najnowsza, zyskująca na popularności głównie przez urządzenia mobilne metoda, wykorzystująca dane biometryczne użytkownika, przykładowo:
  - Skanery odcisków palca,
  - Skanery siatkówki,
  - Rozpoznawanie twarzy.

Metody te stosowane mogą być samodzielnie, lub w połączeniu ze sobą, tworząc rozwiązania autentykacyjne, z których najpopularniejsze to:

- **Login + Hasło** - Najprostszy sposób autentykacji, oparty wyłącznie na wiedzy użytkownika. Jego główną zaletą jest prostota implementacji i wygoda wykorzystania, ponieważ nie wymaga fizycznych poświadczeń tożsamości. Rozwiązanie to jednak nie należy do najbezpieczniejszych, ponieważ przejęcie danych użytkownika umożliwia uzyskanie dostępu do systemu,
- **Weryfikacja dwuetapowa** - Połączenie informacji użytkownika, z informacjami które posiada, najczęściej w formie Login + Hasło + Kod Autentykacyjny. Popularne rozwiązanie stosowane w wielu serwisach internetowych, które po zalogowaniu użytkownika przy pomocy jego informacji, wymaga podania dodatkowego kodu do uzyskania autentykacji w systemie. Rozwiązanie to zapewnia znaczący wzrost bezpieczeństwa w stosunku do klasycznego logowania, kosztem wygody użytkowania, oraz większej trudności implementacji. Największym związanym z nim problemem jest utrata dostępu w momencie utraty urządzenia wykorzystywanego do autentykacji, jednak wiele usług oferuje dodatkowe zabezpieczenie w formie tzw. backup codes - jednorazowych kodów które mogą być wykorzystane w przypadku braku dostępu do urządzenia autentykującego,

- **SmartCard + Hasło** - Metoda wykorzystywana często w systemach firmowych, po wprowadzeniu karty do czytnika użytkownik jest rozpoznawany i proszony o podanie przypisanego do jego konta hasła. Metoda ta zapewnia optymalny poziom bezpieczeństwa, jednak utrata dostępu do karty wymaga utworzenia jej duplikatu, a zazwyczaj również resetu hasła.

1.2 Mechanizmy ochrony danych w systemach operacyjnych

Ponieważ podstawowym zadaniem systemu operacyjnego jest zapewnienie możliwości (pseudo)-równoczesnego wykonywania wielu procesów użytkownika – czyli uruchomionych w systemie programów – istotne jest zabezpieczenie przed wzajemnym czytaniem lub nadpisywaniem pamięci systemowej (RAM) przez różne procesy. We współczesnych systemach ten rodzaj ochrony jest zapewniany przez **wirtualizację pamięci** (chociaż nie jest to jedyny jej cel).

W systemie ze stronicowaną pamięcią wirtualną, każdy proces posiada swoją własną przestrzeń adresową, której rozmiar zależy od długości słowa maszynowego (w przypadku procesorów i systemów 64-bitowych – 264 bajtów) i generalnie może być znacznie większy od rozmiaru pamięci zainstalowanej fizycznie. Stosowane w takiej wirtualnej przestrzeni adresowej przez programy **adresy logiczne** są tłumaczone przez system operacyjny na **adresy fizyczne** dzięki **tablicom stron**, przechowującym informację o przyporządkowaniu określonych fragmentów przestrzeni adresowej procesu (stron) do odpowiednich fragmentów pamięci fizycznej (ramek). Aby utrudnić ataki na oprogramowanie za pomocą exploitów, dodatkowo może zostać zastosowana **randomizacja przestrzeni adresowej** (ang. ***ASLR*** – *Adress Space Layout Randomization*). Polega ona na losowym rozmieszczaniu kluczowych obszarów (np. segmentu danych i segmentu stosu) w wirtualnej przestrzeni adresowej procesu, dzięki czemu atakującemu trudniej jest przewidzieć, w którym miejscu powinien podłożyć potrzebne do dokonania ataku dane (np. spreparowany adres powrotny z funkcji).

Zabezpieczenia pamięci czasami da się obejść wykorzystując podatności architektury procesora, takie jak odkryte w 2018 roku różne warianty ataku **Spectre**, na które procesory podatne są w różnym stopniu – w przypadku architektury x86 generalnie procesory firmy Intel podatne są na więcej wariantów niż procesory firmy AMD, ale problem dotyczy też innych architektur (np. ARM). Ataki te polegają na odpowiednim wykorzystaniu chybień **spekulatywnego wykonywania kodu** – czyli wykonywania przez część jednostek procesora fragmentu kodu, do którego może nastąpić skok, zanim będzie wiadomo czy rzeczywiście ten skok nastąpi – do pośredniego odczytywania przez zawartość różnych buforów procesora danych z pamięci, do których nie powinno być dostępu. Skutecznie wykonany atak **Spectre** może np. umożliwić wyciek kluczy kryptograficznych.

Innym zadaniem realizowanym przez system operacyjny jest ochrona danych przechowywanych w pamięci masowej (na dysku) przed dostępem przez różnych użytkowników. Służą do tego uprawnienia na poziomie systemu plików:

- **w systemach uniksowych (m. in. Linux)** – każdy plik ma przypisanego właściciela zwykłego (konto użytkownika) i właściciela grupowego (grupę użytkowników) oraz istnieją, nie licząc kilku specjalnych, trzy rodzaje uprawnień – do odczytu (r), zapisu (w) i wykonania (x) – które podstawowo przydziela się osobno dla właściciela, właściciela grupowego i wszystkich pozostałych użytkowników, a jeżeli taki podział nie jest wystarczający – można wykorzystać listy ACL, które pozwalają te same uprawnienia przydzielać dowolnym innym użytkownikom lub grupom,
- **w systemie Windows z systemem plików NTFS** – każdy plik ma przypisanego właściciela (użytkownika albo grupę), istnieje pięć podstawowych rodzajów uprawnień (pełna kontrola, modyfikacja, wykonanie, odczyt, zapis) i wiele rodzajów specjalnych (np. przejęcie na własność), które przydziela się dla konkretnych użytkowników lub grup za pomocą list ACL, oprócz tego występuje dość skomplikowane dziedziczenie uprawnień w hierarchii katalogów.

1.3 Problem komputerowo wspomaganej diagnostyki medycznej i metody budowy algorytmów diagnostycznych

W procesie diagnostyki medycznej wyróżnia się trzy zasadnicze etapy, nazywane typami decyzji klinicznych:

- **Diagnoza** - Określenie tego, co wiemy o pacjencie - stan początkowy, rozpoznane charakterystyczne cechy, objawy chorobowe
- **Proces diagnostyczny** - Wybór odpowiednich badań, pytań i testów, wraz z uwzględnieniem ich zasadności, ryzyka, kosztów i wymaganego czasu
- **Zarządzanie (terapia)** - Zaplanowanie procesu leczenia, nadzorowanie go, weryfikacja postawionej diagnozy

W procesie diagnostyki, systemy komputerowe mogą dostarczyć informacji w dwojaki sposób:

- **Pośrednio** - System dostarcza informacyjne zasoby medyczne, umożliwiające specjaliście łatwą analizę i wyszukiwanie informacji, w celu stawiania trafniejszych diagnoz i szybszego uzyskiwania danych dotyczących pacjenta, jego objawów i potencjalnych schorzeń. Przykładem takiego rodzaju systemu jest Rejestr Przypadków Medycznych, zawierający opisy pacjentów, wraz z postawionymi diagnozami i skutkami terapii.
- **Bezpośrednio** - Na podstawie odpowiednio zapisanej wiedzy medycznej, system sam wyznacza diagnozę dla pacjenta, wykorzystując już gotowe modele decyzyjne, bądź przeprowadzając ekstrakcję danych i tworząc model decyzyjny na ich podstawie. Przykładem takiego systemu może być ISABEL, którego twórcy chwalą się poprawnością diagnoz na poziomie 96

W publikacji badawczej *Ten commandments for effective clinical decision support: making the practice of evidence-based medicine a reality*, zdefiniowane zostało 10 podstawowych założeń jakie spełniać powinny systemy bezpośredniej diagnostyki medycznej. Na ich podstawie określić można główne problemy, z jakimi zmagać się muszą autorzy takich systemów:

- **Duża ilość zmiennych w procesie analizy** - Ilość informacji jakie analizowane są w procesie diagnostyki medycznej jest bardzo duża, a powiązania pomiędzy nimi nie zawsze da się w jasny sposób określić. Ciężko jest również przeprowadzić selekcję istotnych cech, ponieważ eliminowanie czynników wykonywane musi być bardzo ostrożnie, aby uniknąć pozbycia się istotnych danych. Przykładowo, usunięcie informacji o alergii pacjenta na jedną z substancji może skutkować podaniem leku, który doprowadzi do jego śmierci.
- **Wydajność i złożoność obliczeniowa** - W diagnostyce medycznej istotnym czynnikiem jest czas, decyzje często podejmowane muszą być bardzo szybko, więc systemy nie mogą przeprowadzać analizy w sposób nieoptymalny, oraz muszą potrafić reagować bardzo szybko w sytuacjach kryzysowych. Przykładowo, jeżeli pacjent dostaje nagłego ataku, system musi określić podanie odpowiedniego środka zapobiegawczego w możliwie najkrótszym czasie, uwzględniając jego alergie, wydolność organizmu itp.
- Konieczność dopasowywania się do sytuacji - System musi umieć dopasować się do dostępnego w danej placówce sprzętu i zakresu substancji leczniczych, znajdując alternatywne sposoby terapii. Dopasowywanie się powinno również uwzględniać zmianę decyzji w oparciu o działania przeprowadzone przez lekarza poza systemem. Przykładowo: System proponuje podanie leku A, jednak lekarz decyduje się na podanie leku B. W takim wypadku, system powinien potrafić określić dalsze kroki postępowania, w oparciu o lek B, a nie A. Jeżeli nie będzie w stanie tego zrobić, stanie się bezużyteczny w dalszym procesie leczenia.
- **Wyszukiwanie najprostszego rozwiązania** - System powinien być w stanie wyznaczyć terapię, która zaproponuje rozwiązanie problemu medycznego w najprostszy sposób, aby ograniczyć nie tylko zużycie zasobów medycznych i czas leczenia, ale również zasoby finansowe. Przykładowo, w terapii pacjenta cierpiącego na długotrwałą chorobę psychiczną spowodowaną

studiami na Politechnice, system znajduje terapię lekiem A, trwającą rok, oraz terapię lekiem B, trwającą 5 lat. System powinien określić która z nich będzie rozwiązaniem lepszym pod względem czasowym, finansowym oraz zdrowotnym.

- **Utrzymanie i rozwój modeli decyzyjnych** - Ze względu na bardzo częste zmiany informacji i ciągły rozwój badań w dziedzinie medycyny, konieczne jest regularne aktualizowanie i weryfikowanie działania modeli decyzyjnych wykorzystywanych do rozpoznawania i diagnozowania chorób. Przykładowo: pojawia się COVID-19, jeżeli nie zostanie on wprowadzony do bazy informacji oraz odpowiednio scharakteryzowany, system nie będzie w stanie go rozpoznać oraz zaproponować odpowiedniej diagnostyki.

1.4 Zadania komputerowego przetwarzania biosygnałów na wybranym przykładzie (np. EKG, EMG)

Zależnie od źródła pochodzenia, wyróżnić można kilka rodzajów sygnałów biomedycznych:

- **Mechaniczne** - Np. ciśnienie krwi, ruchy wykonywane przez organy lub części ciała, sygnały dźwiękowe (przykładowo szmery w układzie oddechowym),
- **Chemiczne** - Np. współczynnik PH płynów ustrojowych, zawartość określonej substancji składowej,
- **Termiczne** - Np. ciepło emitowane przez poszczególne części ciała,
- **Elektryczne** - Np. EKG, EMG (pochodzące z serca), EEG (pochodzące z układu nerwowego),
- **Magnetyczne** - Powiązane z sygnałami elektrycznymi, ale rzadko wykorzystywane ze względu na trudność ich rejestracji i identyfikacji.

Zależnie od stochastyki, podzielić je można natomiast na dwie podgrupy:

- **Stacjonarne** - Statystyczne parametry tych sygnałów nie ulegają zmianie. Przykładowo: norma zawartości żelaza we krwi określana jest odgórnie zależnie od wymiarów organizmu, więc wartość oczekiwana tego parametru nie ulega zmianie w czasie,
- **Niestacjonarne** - Statystyczne parametry tych sygnałów mogą ulec zmianie w czasie. Przykładowo: wariancja wyznaczana na sygnale EKG lub EEG.

Do najpopularniejszych metody wykorzystywanych w procesie przetwarzania takich sygnałów należą:

- **Filtracja** – Usuwanie lub redukcja pewnych elementów sygnału,
- **Analiza** – Ekstrakcja poszukiwanych cech z sygnału, zazwyczaj poprzez jego segmentację lub parametryzację, pozwalając na konwersję sygnału do postaci wektora cech, który poddany zostać może dalszej analizie,
- **Interpretacja** - Porównanie otrzymanego pomiaru z oczekiwanym wzorcem, wyszukiwanie w nim anomalii lub charakterystycznych elementów.

1.4.1 Przykładowa analiza sygnału EKG

Sygnał EKG jest napięciem elektrycznym rejestrowanym na ciele poprzez odpowiednio połączone elektrody. Pozwala on zdiagnozować liczne problemy powodowane przez choroby serca, lub zaburzenia jego pracy. Jest on jednym z najczęściej wykorzystywanych i najlepiej zbadanych sygnałów wykorzystywanych w diagnostyce medycznej. Analiza tego sygnału przeprowadzana jest w trzech etapach:

- **Filtracja** - Usuwa określone pasma z pomiaru:
  - **Filtr górnoprzepustowy** - Usuwania dryft linii izoelektrycznej (0.2Hz – 0.5Hz),
  - **Filtr szczelinowy** - Usuwa zakłócenia sieci elektroenergetycznej (50Hz),
  - **Filtry dolnoprzepustowe** - Usuwają zakłócenia pochodzące z drżeń mięśniowych, aparatury elektromedycznej, oraz artefakty pomiaru (25Hz, 35Hz).
- **Analiza** - Wyznacza charakterysytyczne punkty sygnału (początek i koniec P, QRS, koniec T, lokalizacja Q, R, S, J, amplitudy P, Q, R, S, T, nachylenie S-T) oraz parametry zespołu uśrednionego (uśrednione wartości tych samych charakterystyk dla kilku różnych sygnałów EKG),
- **Interpretacja** - Porównanie cech otrzymanego sygnału (np. odstęp PQ, czas trwania zespołu QRS, amplituda załamka Q, nachylenie odcinka ST) z kryteriami medycznymi dla rożnych zaburzeń (np. blok przedsionkowo-komorowy, rytm nadkomorowy, przerost lewej komory, itp.).

1.5 Metody i narzędzia wykorzystywane w opisywaniu procesów biznesowych

W zagadnieniach związanych z opisywaniem procesów biznesowych, wykorzystywane są różne rodzaje podstawowych procesów zarządzania, określone w *Podnoszenie efektywności organizacji*:

- **Ogólne procesy podstawowe** (np. zakładanie nowego biznesu, przygotowanie i wprowadzenie nowego produktu, produkcja, obsługa pogwarancyjna),
- **Procesy podstawowe specyficzne dla branży** (np. załatwianie wniosku kredytowego, rozpatrzenie wniosku o odszkodowanie, stworzenie programu),
- **Ogólne procesy wspierające** (np. formalne planowanie strategiczne i taktyczne, budżetowanie, rekrutacja, szkolenie),
- **Ogólne procesy zarządzania** (np. planowanie strategiczne i taktyczne, ustalanie celów, alokacja zasobów).

W zależności od specyfiki organizacji i branży, wybrać można różne technologie pozwalające na zarządzanie procesami biznesowymi.

1.5.1 BPMN - Business Process Modelling Notation

Graficzny język wizualizacji, specyfikowania, tworzenia i dokumentowania procesów biznesowych. Służy do opisu procesów na potrzeby systemów ERP (zarządzanie zasobami w przedsiębiorstwach) oraz WorkFlow (obieg pracy, dokumentów). Celem BPMN jest wymiana procesów biznesowych na poziomie ludzi zamiast poziomu technicznego. Wspiera proste i złożone procesy, oraz prostą wymianę komunikacji między użytkownikami - podstawą są diagramy procesów biznesowych. BPMN tworzy most między notacją pojęciową i techniczną - przekształca pomysł na kod (np. język BPL). Proces biznesowy w BPMN to zaplanowany proces (zbiór wzajemnie powiązanych działań, które przekształcają elementy wejściowe na wyjściowe) nastawiony na uzyskiwanie określonych rezultatów. BPMN koncentruje się na sekwencji procesu z trzema rodzajami podprocesów:

- **Prywatne** (Wewnętrzne procesy biznesowe) - Wykonywane są wewnątrz jednostki organizacyjnej (w ogólnych przepływach pracy procesów BPM),
- **Publiczne** (Abstrakcyjne procesy)- ilustrują interakcję między wewnętrznymi procesami a zewnętrznymi partnerami biznesowymi (wskazując sekwencję interakcji/wiadomości wewnętrznego procesu z zewnętrznymi użytkownikami). Ponadto przedstawiane są tylko czynności obejmujące zewnętrzną komunikację (wskazując przepływ sterowania),
- **Globalne** (Procesy współpracy) - ilustrują interakcje między dwoma lub więcej partnerami biznesowymi. Sekwencja czynności pokazuje wymianę wiadomości między jednostkami.

1.5.2 BPEL - Business Process Execution Language for Web Services

Język zorientowany na procesy i wykonanie takiego zapisu w specjalizowanym silniku. Został opracowany m.in. przez IBM i Microsoft. Jest to przede wszystkim język do definiowania procesów biznesowych w usługach sieciowych. BPEL zawiera zarówno warstwę abstrakcyjną (definiowane są w niej parametry i ograniczenia), jak i warstwę niskiego poziomu (definiowane są w niej wykonywalne procesy). Najpopularniejsze implementacje tego języka to Microsoft BizTalk oraz JBoss jBPM.

1.5.3 BPML - Business Process Management Language

Konkurent dla BPEL, opracowany przez Business Process Management Initiative. Pozwala na automatyczne tłumaczenie postaci graficznej do kodu konkurencyjnego języka BPEL. Pod względem działania nie różni się znacząco od BPEL, jest jednak mniej popularny ze względu na brak tak szerokiego wsparcia jak BPEL

1.6 Problemy bezpieczeństwa transakcji zawieranych przy pomocy komunikacji bezprzewodowej

W sieci bezprzewodowej występuje wiele problemów bezpieczeństwa - w przypadku sieci jesteśmy narażeni na m.in. sniffing, spoofing (SMTP, WWW, ARP, DNS itd.). Ze względu na łatwy dostęp do medium transmisyjnego, przez które następuje wymiana danych łatwiejsze są ataki Main in the Middle, Evil Twin, spoofing MAC, modyfikowanie pakietów, złamanie zabezpieczeń WEP, WPA, podsłuchwanie nieszyfrowanych transmisji.

1.6.1 Man in the Middle

Atak polega na przechwyceniu niezbędnych do wykonania transakcji danych i tym samym kradzieży środków lub tożsamości. W celu wykonania ataku należy przechwycić komunikację pomiędzy osobą atakowaną, a bankiem, następnie przekonać użytkownika, że strona, na którą się loguje (spreparowana przez nas) jest stroną, na którą chce się zalogować. Za pomocą otrzymanych danych można uzyskać dostęp od konta użytkownika.

Aby uchronić się przed tym atakiem należy sprawdzać certyfikaty stron podczas wykonywania transakcji, nie wykonywać transakcji będąc podłączonym do sieci publicznej. Banki, aby się przed tym bronić wprowadziły weryfikację SMS, w treści SMS możemy zweryfikować numer konta bankowego oraz kwotę przelewu.

1.6.2 Sniffing transmisji

Atak polega na podsłuchiwaniu transmisji nieszyfrowanych, dzięki czemu możliwe jest uzyskanie danyh takich jak login czy hasło do różnych systemów komputerowych, co pozwala na podszywanie się pod atakującą osobę. Aby dokonać ataku wystarczy oprogramowanie pozwalajace na to (np. Whireshark) lub odpowiendio skonfigurowana karta sieciowa.
Aby uchronić się przed tym atakiem można skonfigurować sieć, aby wymuszała szyfrowanie danych, nawiązywanie komunikacji w wyższych warstwach sieci w sposób szyfrowany np. TLS 1.1, SSL.

1.6.3 Evil Twin

Atak polega na podstawieniu urządzenia (np. WiFi Pineapple) , które symuluje Access Point. W przypadku, gdy urządzenie zacznie wygłaszać mocniejszy sygnał od prawdziwego nastąpi przełączenie bez informowania użytkownika. Dzięki temu cały ruch z komputera będzie przechodził przez fałszywy Access Point, co daje możliwość łatwego przechwycenia danych.

Będąc na konferencji niebezpiecznika pokazywali urządzenie WiFi Pineapple, którego używają do pentestów. Gdy w telefonie zostaje włączone WiFi, telefon wyszukuje dostępne wokół niego sieci oraz odpytuje je "czy jesteś zapamiętaną przeze mnie siecią x?", a urządzenie WiFi Pineapple zawsze odpowiada "TAK", dzięki czemu telefon się łączy z fake'owym Access Pointem.

W celu ochrony należy łączyć się tylko ze sprawdzonymi sieciami, wykorzystywać zabezpieczoną komunikację, oraz wyłączać WiFi w telefonie, gdy go nie używamy.

1.6.4 Spoofing MAC

Jedną z metod zabezpieczenia dostępów do sieci bezprzewodowej jest weryfikacja urządzeń po adresie fizycznym karty sieciowej MAC. Jednak podsłuchiwanie transmisji w sieciach bezprzewodowych jest stosunkowo proste, dlatego jest możliwość odczytania adresów MAC urządzeń, które mają

dostęp do danych zasobów, a następnie podmienienie własnego adresu fizycznego MAC na jeden z nich.

Aby uchronić się przed tym atakiem należy oprócz weryfikacji adresów MAC używać zabezpieczeń hasłem lub nadawanie dostępu do zasobów dla użytkowników z dostępem do lokalnej sieci.

1.6.5 Złamanie zabezpieczeń WEP i WPA

Zabezpieczenia za pomocą WEP i WPA są mało bezpieczne, przy odpowiednim ataku możliwe jest zgadnięcie w ciągu kilkunastu/kilkudziesięciu minut (np. za pomocą narzędzia AirSnort). Dlatego należy używać lepszych zabezpieczeń - najskuteczniejszym obecnie szyfrowaniem jest WPA2, które używa algorytmu Advanced Encryption Standard (AES).

1.6.6 Modyfikowanie pakietów

W przypadku przechwycenia transmisji możliwe staje się zmodyfikowanie adresów, z którego została wysłana wiadomość, przez co możliwe staje się przechwycenie odpowiedzi serwera. Aby zabezpieczyć się przed modyfikowaniem pakietów konieczne jest zapewnienie integralności pakietów i jej weryfikacja.

1.6.7 Przechwytywanie sygnału bluetooth

Temat dotyczy komunikacji bezprzewodowej, więc również bluetooth.

Problem dotyczy klawiatur bezprzewodowych. Atakujący może dysponować urządzeniem, które będzie przechwytywało wciśnięte przez użytkownika przyciski, co po odpowiedniej analizie pozwoli na wyodrębnienie loginów i haseł.

Problemy z bezpieczeństwem RFID - można łatwo zczytać kartę, sklonować ją.

1.7 Analiza systemów informatycznych z użyciem sieci Petriego

Sieci Petriego – jest to matematyczna reprezentacja systemów rozproszonych. Umożliwiają one badanie zjawisk współbieżnych zachodzących w systemach wzajemnie się warunkujących w czasie. Uogólniają one teorię automatów. Podstawowa wersja sieci Petriego składa się z:

- **miejsc** (odpowiadających warunkom),
- **przejść** (odpowiadających zdarzeniom),
- **łuków** (krawędzi, odpowiadających związkom między zdarzeniami i warunkami.

Aby opisać konkretny stan układu, potrzebne są żetony które można przemieszczać pomiędzy miejscami poprzez przejścia po krawędziach grafu. Oznaczeniami są:

- **kropki** – żetony
- **prostokąty**(grube kreski) – przejścia
- **okręgi** – miejsca
- **strzałki** – krawędzie, łuki

Działanie sieci polega na przesuwaniu się znaczników między miejscami sieci.

1.7.1 Własności sieci Petriego

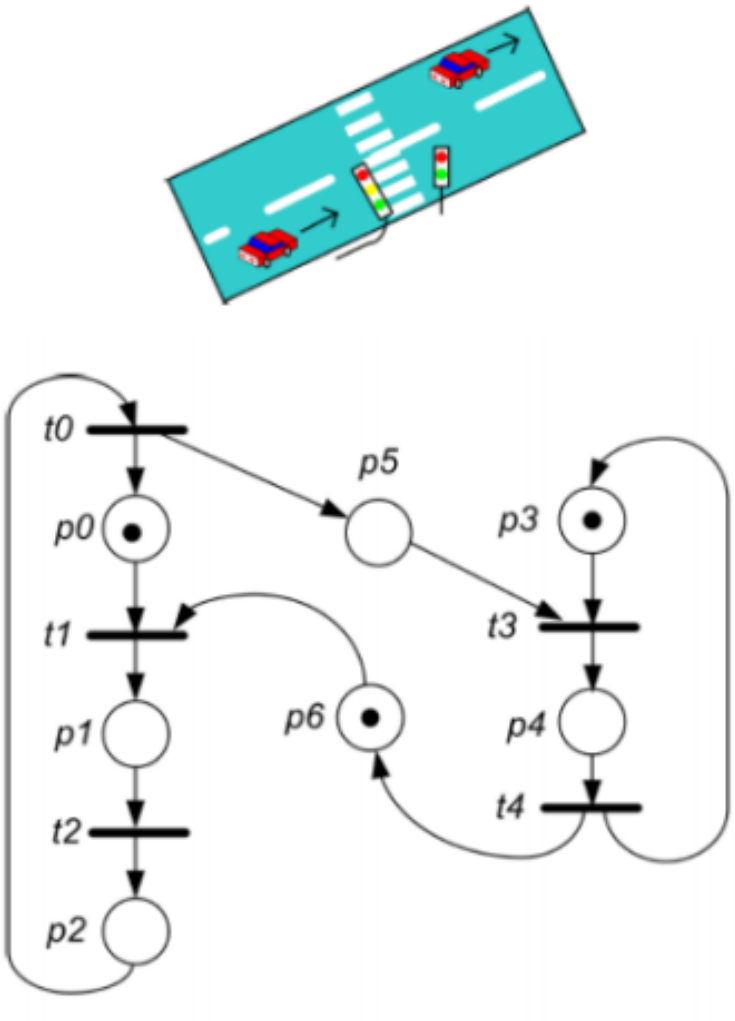
- **Osiągalność** – sprawdzanie, czy dany stan jest osiągalny ze stanu początkowego (tzn. czy istnieje skończona liczba przejść, która prowadzi od znakowania początkowego do znakowania badanego).
- **Ograniczoność** – liczba znaczników w danym miejscu jest ograniczona.
- **Zachowawczość** – sieć Petriego jest zachowawcza, jeżeli liczba występujących w niej znaczników jest stała.
- **Żywotność** – określa liczbę możliwych wykonań przejścia. Sieć jest żywa, jeżeli z każdego oznakowania można osiągnąć inne oznakowania.
- **Odwracalność** – sieć jest odwracalna, jeżeli stan początkowy sieci jest osiągalny z każdego oznakowania.

Trzy główne metody analizy sieci Petriego:

- **Grafy osiągalności** – opiera się ona na budowie drzewa osiągalności. Ze stanu początkowego odpala się wszystkie możliwe przejścia , które prowadzą do osiągalnych znakowań tworzących węzły grafu, z nich tworzone są kolejne, itd. W drzewie osiągalności można w sposób jednoznaczny dojść od korzenia do dowolnego innego węzła. Drzewo może być nieskończone.
- **Grafy pokrycia** - otrzymywany jest z drzewa pokrycia poprzez scalenie duplikujących się wierzchołków. Na podstawie skończonego grafu pokrycia możliwe jest badanie sieci o nieskończonym zbiorze znakowań.
- **Metody algebraiczne** (macierz incydencji). Definiuje się macierz wejść wyjść. W macierzy incydencji liczba wierszy to liczba miejsc, liczba kolumn to liczba przejść.

1.7.2 Przykład sieci Petriego

Chcemy zaprojektować oprogramowanie dla systemu kontroli sygnalizacji świetlnej. Zakładamy, że dane są dwa autonomiczne systemy sterujące sygnalizacją świetlną – jeden dla pojazdów i drugi dla ludzi. Należy je zsynchronizować.



Rysunek 1: Przykładowa sieć

Znaczenie miejsc na rysunku 1.3 jest następujące:

- p0, p1, p2 – światła uliczne dla aut, odpowiednio p0 – czerwone, p1 – żółte, p2 – zielone,
- p3, p4 – światła uliczne dla pieszych, odpowiednio p3 – czerwone, p4 – zielone,
- p5, p6 – miejsca służące do synchronizacji (np. flagi umieszczone w oprogramowaniu).

1.8 Weryfikacja modelowa z zastosowaniem logiki temporalnej

Logika temporalna jest to rozszerzenie logiki tradycyjnej o symbole określające upływ czasu. Weryfikacja modelowa pozwala odpowiedzieć na pytanie czy formalny model funkcji systemu dany jako automat spełnia własności, zdefiniowane za pomocą formuł logiki temporalnej. Główne zastosowania to:

- zarządzanie temporalnymi bazami danych,
- opis systemów współbieżnych,
- opis systemów reagujących na bodźce,
- określanie własności systemów,
- automatyczna weryfikacja programów – matematyczne udowodnienie ich poprawności.

Najważniejsze zadania weryfikacji:

- osiągalność (pożądany stan zostanie **w końcu** osiągnięty)
- bezpieczeństwo (gwarancja, iż stan nieprawidłowy **nigdy** nie zostanie osiągnięty)

1.8.1 Typy logiki temporalnej

Wyróżniamy 3 typy logiki temporalnej:

- **LTL** (*Linear Temporal Logic*) – z liniową strukturą czasu,
- **CTL** (*Computation Tree Logic*) – rozszerzenie logiki LTL o rozgałęzione warianty upływu czasu). Czas jest dyskretny, może się rozgałęziać (ale od pewnego momentu, wcześniej jest liniowy) oraz lewostronnie skończony (w przyszłości nieskończony). Zastosowanie : w działających współbieżnie programach , w systemach gdzie istnieje wiele wariantów upływu czasu,
- **Real Time CTL** - dalsze rozwiniecie logiki temporalnej, pozwala na weryfikacje systemów czasu rzeczywistego, gdzie dana operacja nie tylko musi być wykonana, ale też są na nią ograniczone ramy czasowe.

1.8.2 Zalety i wady

Zalety:

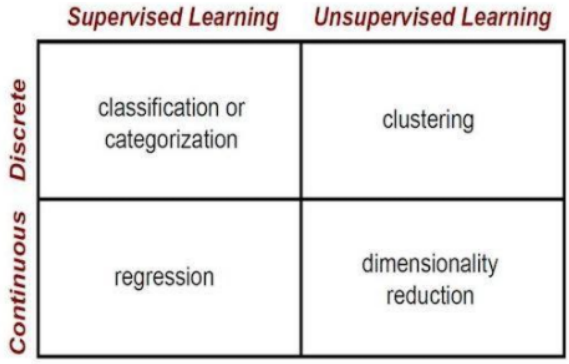
- pełna automatyzacja (po utworzeniu wymagań i zdefiniowaniu ograniczeń wystarczy uruchomić weryfikację),
- łatwe dowodzenie nieprawidłowości przez znalezienie kontrprzykładu.

Wady

- złożoność obliczeniowa;eksplozja stanów,
- wykonanie abstrakcji wymaga pracy eksperta.

2 Pytania Specjalnościowe

2.1 Uczenie nadzorowane i nienadzorowane - charakterystyka, metody i zastosowania



Rysunek 2: TLDR

2.1.1 Charakterystyka

Uczenie nadzorowane

Jeżeli zbiór danych zawiera pary składające się z: **wejściowego obiektu uczącego** (np. wektor) oraz **pożądaną odpowiedź** (np. klasę), to mamy do czynienia z **uczeniem nadzorowanym**.

Załóżmy, że znamy wartości pomiarów (X) i oraz klasyfikację/ocenę pomiarów (Y). Do klasyfikacji możemy posłużyć się mapowaniem: $Y = f(X)$. Celem uczenia nadzorowanego jest wyznaczenie funkcji f potrafiącej wyznaczyć klasyfikację Y dla dowolnych pomiarów X spoza posiadanego zbioru uczącego.

Proces nauki polega na iteracyjnym przetwarzaniu próbek treningowych. Dla każdej próbki wyznaczany jest błąd predykcji, definiujący jak bardzo predykowana wartość różni się od rzeczywistej. Dzięki „nauczycielowi" model uczy się poprawnie wyznaczać **pożądaną odpowiedź**, co jest charakterystyczne dla tego rodzaju uczenia. Proces nauki trwa do momentu wyznaczenia akceptowalnego poziomu błędu. Skuteczność wyuczonego modelu można sprawdzić poprzez np. wyznaczenie predykcji dla zbioru testowego.

Przykłady zastosowania: zarządzanie ryzykiem; wykrywanie nadużyć; personalizacja interakcji; rozpoznawanie mowy, tekstu i obrazu oraz segmentacji klientów.

Uczenie nienadzorowane

Jeżeli zbiór danych sieci neuronowej zawiera **wejściowy obiekt uczący** (np. wektor), ale **NIE ZAWIERA pożądanej odpowiedzi** (np. klasę), wówczas mamy do czynienia z **uczeniem nienadzorowanym**.

Ponieważ zbiór danych nie posiada pożądanej odpowiedzi, model nie otrzymuje instrukcji co on właściwie ma zrobić z uzyskanymi danymi. Brak gotowych klas definiuje cel uczenia nienadzorowanego – zrozumieć i zdefiniować strukturę próbek wejściowych. Uczenie nienadzorowane polega na

modelowaniu rozkładu danych, w celu uzyskania dodatkowych informacji na temat relacji między danymi wejściowymi.

Przykłady zastosowania: analiza koszyka zakupowego, wykrywanie anomalii, rozpoznawanie podobnych obiektów.

Uczenie częściowo nadzorowane

W tym przypadku maszyna otrzymuje zarówno **dane wejściowe oznaczone** (zawierające odpowiadające im dane wyjściowe, konkretne przykłady), jak i **nieoznaczone** (wymagające przyporządkowania do danych wyjściowych, znalezienia odpowiedzi). Ten rodzaj uczenia maszynowego wykorzystuje się w sytuacjach, gdy organizacja dysponuje zbyt dużą ilością danych lub gdy informacje są na tyle zróżnicowane, że nie sposób przyporządkować odpowiedzi do każdej z nich. System sam proponuje odpowiedzi i jest w stanie stworzyć ogólne wzorce.

Przykłady zastosowania: rozpoznawanie mowy i obrazu, klasyfikacja stron internetowych.

Uczenie wzmocnione

Maszyna otrzymuje gotowy zestaw **dozwolonych działań, reguł i stwierdzeń**. Działając w ich ramach, dokonuje analizy i obserwuje ich skutki. Wykorzystuje reguły w taki sposób, aby osiągnąć pożądany efekt. Można to porównać do nauki gry np. w koszykówkę. Zasady określające, kiedy są kroki, faul czy aut pozostają niezmienne. Natomiast to, w jaki sposób drużyna zdobędzie punkt (zawodnik rzuci z dystansu, wbiegnie pod kosz lub poda) zależy od decyzji graczy, którzy podejmują ją na bieżąco.

Przykłady zastosowania: nawigacja (wybór trasy na podstawie informacji o natężeniu ruchu i warunkach na drodze), gaming (dostosowywanie scenariuszy rozgrywki do działań gracza), robotyka (dostosowanie pracy robotów do obłożenia i rodzaju wytwarzanego produktu).

2.1.2 Zadania uczenia maszynowego

Zadanie uczenia maszynowego – abstrakcyjny opis problemu, który możemy rozwiązać przy użyciu uczenia maszynowego. Zadania uczenia maszynowego nazywamy często problemami uczenia maszynowego. Wyróżniamy następujące zadania:

Uczenie nadzorowane

- **Klasyfikacja** – przyporządkowanie klas do obiektów pochodzących z pewnego zbioru. Wyróżniamy:
  - **Klasyfikację jednoklasową** – identyfikowanie obiektów o ustalonej klasie;
  - **Klasyfikację binarną** – klasyfikacja obiektów do jednej z dwóch klas;
  - **Klasyfikację wieloklasową** – przyporządkowanie obiektowi klasy pochodzącej ze zbioru składającego się z co najmniej 3 klas. Klasyfikacja wieloklasowa może zostać zredukowana do wielokrotnej klasyfikacji binarnej przy użyciu jednej z dwóch strategii:
    - **Jeden przeciw wszystkim** – binarna klasyfikacja dla każdej z N klas, zestawiona z klasą powstał przez połączenie pozostałych N-1 klas;
    - **Jeden przeciw jednemu** – binarna klasyfikacja pomiędzy wszystkim z N rozważanych klas.

  - **Klasyfikacja wieloetykietowa** – przyporządkowanie kilku etykiet/klas do każdego z klasyfikowanych obiektów.
- **Regresja** – przyporządkowanie obiektom wartości liczbowych. Analogicznie jak przy zadaniu klasyfikacji, tylko zamiast etykiet używamy liczb rzeczywistych.

Uczenie nienadzorowane

- **Klasteryzacja** – grupowanie obiektów o podobnych cechach. Podobieństwo obiektów jest wyrażenie przy użyciu pojęć takich jak: dystans czy metryki podobieństwa.
- **Reguły asocjacyjne** – wykrywanie relacji pomiędzy zmiennymi opisującymi obiekty. Zwane również „frequent itemset problem".
  - **Reguła**: jeśli X wówczas Y (słynny przykład: „jeśli klienci kupują pieluszki, często kupują również piwo")
  - **Ważne pojęcia:**
    * „**Support**" reguły – procent transakcji zawierających zarówno X jak i Y.
    * „**Confidence**" reguły – procent transakcji zawierających Y spośród tych z X.
  - Szukamy wszystkich reguł z zadanym min **support** i **confidence**.
- **Redukcja wielowymiarowości** – redukcja liczby używanych atrybutów pochodzących ze zbioru uczącego. Na przykład w celu optymalizacji procesu uczenia (przy mniejszej ilości cech łatwiej znaleźć te najbardziej wpływowe). Wyróżniamy:
  - **Selekcja atrybutów** – redukcja zbioru uczącego do podzbioru z najważniejszymi atrybutami (selekcja np. na podstawie przyrostu informacji).
  - **Ekstrakcja atrybutów** – łączenia atrybutów przy pomocy operacji liniowych bądź nieliniowych i tworzenie nowych atrybutów łączących cechy wspólne.

2.1.3 Metody

Uczenie nadzorowane

- **Regresja logistyczna** – (wbrew nazwie) liniowy model używany częściej do klasyfikacji niż regresji.
- **Naiwny Bayes** – klasyfikator prohabilistyczny, zakładający niezależność parametrów klasy względem siebie.
- **SVM** – abstrakcyjny koncept maszyny, której nauka ma na celu wyznaczenie hiperpłaszczyzny rozdzielającej z maksymalnym marginesem należące do dwóch klas.
- **Sieci neuronowe** – systemy komputerowe, strukturą zainspirowane naturalnymi neuronami. Składa się z szeregów neuronów, przekształcających matematycznie próbki wejściowe do zrozumiałej postaci.
- **Random (decision) forests** – to metoda uczenia się przez wzmacnianie. Działają poprzez konstruowanie wielu drzew decyzyjnych. Każde drzewo dokonuje osobistej, niezależnej predykcji. Odpowiedzią lasu zależy od implementacji lasu i może to być m.in. średnia (ważona) odpowiedzi.

Uczenie nienadzorowane

Klasteryzacja:

- **k-means clustering** – cel K-średnich jest prosty: zgrupuj podobne punkty danych razem i odkryj wzorce. Aby osiągnąć ten cel, K-średnich szuka stałej liczby k klastrów w zbiorze danych. Klaster odnosi się do zbioru punktów danych agregowanych ze względu na pewne podobieństwa. Algorytm wygląda następująco:
  - Wybierz k punktów (początkowe centroidy klastrów)
  - Przypisz każdą obserwację do najbliższego klastra (najbliższego centroida).

  - Dla każdego klastra wyznacz nowy centroid.
  - Powtarzaj krok 2 i 3 tak długo aż żadna obserwacja nie zmieni przynależności do klastra.

Redukcja wymiarów:

- **PCA** (Principal Component Analysis) – biorąc pod uwagę zbiór punktów w przestrzeni dwu, trzy lub większej, linię „najlepiej pasującą" można zdefiniować jako taką, która minimalizuje średnią kwadratową odległość od punktu do linii.
  - Obserwujemy realizację p zmiennych (np. monitoring procesu przemysłowego, zmienne skorelowane)
  - Przekształcamy p zmiennych (na n obserwacjach) w nieskorelowany zbiór p zmiennych – principal components
  - Zmienność w danych opisuje kilka pierwszych komponentów
- **Autoenkoder** – kompresuje dane do postaci reprezentacji, a następnie odtwarza wynik. Sieć składa się z:
  - **kodera** (ang. encoder), który przekształca dane wejściowe do postaci reprezentacji,
  - **dekodera** (ang. decoder), który przekształca dane z postaci reprezentacji do danych wyjściowych

Reguły asocjacyjne:

- **Algorytm a priori**
  - Spostrzeżenie: zbiór X jest częsty -> każdy podzbiór X jest częsty.
  - Dla ustalonego support s znajdź obiekty występujące w co najmniej $s\%$ koszyków (zbiór L 1) – pierwsze przejście przez dane (tablica liczników częstości dla obiektów zmieści się w RAM)
  - Zbiór par obiektów z L 1 stanowi zbiór kandydatów na częste pary C 2 – drugie przejście przez dane – wyznaczenie częstych par L 2
  - Z L 2 tworzymy C 3 (kandydaci na częste trójki) – stąd L 3 – częste trójki, itd.

2.1.4 Zastosowania

Uczenie nadzorowane

Wejście	Wyjście	Zastosowanie
Email	Spam (0 / 1)	Filtrowanie spamu
Audio	Transkrypt (tekst)	Przepisywanie podcastów
Zdjęcie użytkownika	Czy to on (0 / 1)	Rozpoznawanie na podstawie zdjęcia
Język polski	Język angielski	Tłumaczenie maszynowe
Reklama + dane użytkownika	Kliknięcie w baner (0 / 1)	Reklamy internetowe
Obraz + dane z radaru	Pozycja innych samochodów	Samojezdne samochody
Zdjęcie budynku	Defekt (0 / 1)	Inspekcja wzrokowa
Dane klienta	Czy spłaci kredyt (0 / 1)	Ryzyko kredytowe
Logi z bankowości internetowej	Czy zwyczajne zachowanie (0 / 1)	Wykrywanie anomali (fraud)
Dane behawioralne z karty kredytowej	Czy weźmie produkt kredytowy	Modele skłonności do zakupu
Historyczne informacje o telefonach	Informacje o której odbierze telefon	Model kontaktu z klientem

Rysunek 3: Przykładowe zastosowania uczenia nadzorowanego

Przykłady zastosowania: zarządzanie ryzykiem; wykrywanie nadużyć; personalizacja interakcji; rozpoznawanie mowy, tekstu i obrazu oraz segmentacji klientów.

Uczenie nienadzorowane

Uczenie się bez nadzoru jest bardzo przydatne w **analizie eksploracyjnej** (*exploratory analysis*), ponieważ potrafi automatycznie identyfikować strukturę danych. Na przykład, jeśli analityk próbuje segmentować konsumentów, wyniki uczenia bez nadzoru mogą być doskonałym punktem wyjścia do ich analizy. W sytuacjach, w których zaproponowanie trendów w danych jest niemożliwe lub niepraktyczne, uczenie się bez nadzoru może zapewnić wstępne spostrzeżenia, które można następnie wykorzystać do przetestowania poszczególnych hipotez.

Redukcja wymiarów (możliwa do uzyskania dzięki metodom nienadzorowanym) odnosi się do metod używanych do reprezentowania danych przy użyciu mniejszej liczby kolumn lub funkcji. Podczas uczenia się reprezentacji chcemy poznać relacje między poszczególnymi funkcjami, umożliwiając nam reprezentowanie naszych danych przy użyciu postaci reprezentacji, łączącej początkowe cechy. Ta „ukryta struktura" jest często reprezentowana przy użyciu znacznie mniejszej liczby funkcji niż początkowo, więc może sprawić, że dalsze przetwarzanie danych będzie o wiele mniej intensywne, i może wyeliminować zbędne funkcje.

Przykłady zastosowania: analiza koszyka zakupowego, wykrywanie anomalii, rozpoznawanie podobnych obiektów.

2.2 Miary jakości modeli predykcyjnych. Techniki dostrajania i wyboru modelu

2.2.1 Macierz błędu/ macierz konfuzji/Macierz kontyngencji/Confusion matrix

Macierz N×N, gdzie wiersze odpowiadają poprawnym klasom decyzyjnym, a kolumny decyzjom przewidywanym przez klasyfikator. Liczba n-ij na przecięciu wiersza i oraz kolumny j to liczba przykładów z klasy i-tej, które zostały zaklasyfikowane do klasy j-tej. Budowa dla klasyfikacji binarnej:

	Klasyfikacja pozytywna	**Klasyfikacja negatywna**
Stan pozytywny	Prawdziwie dodatnia (ang. *true positive*, TP)	Fałszywie ujemna (ang. *false negative*, FN)
Stan negatywny	Fałszywie dodatnia (ang. *false positive*, FP)	Prawdziwie ujemna (ang. *true negative*, TN)

Tablica 1: Tablica pomyłek, możliwe wyniki klasyfikacji binarnej

2.2.2 Miary dokładności

- **Dokładność** - procent poprawnych klasyfikacji, opisanych wzorem 1:

$$\textbf{accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

- **Czułość** - stosunek prawidłowych wyników pozytywnych do sumy prawidłowych wyników pozytywnych oraz błędnych wyników negatywnych, który można rozumieć jako zdolność modelu do poprawnego etykietowania(patrz wzór 2),

$$\textbf{recall} = \frac{TP}{TP + FN} \tag{2}$$

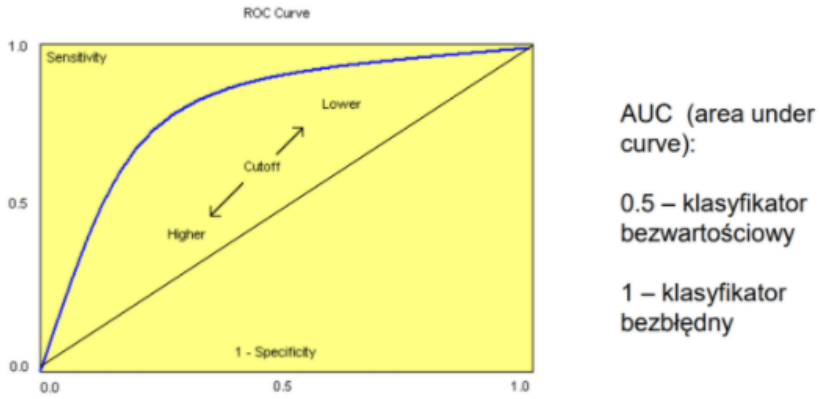
- **Precyzja** - stosunek prawidłowych wyników pozytywnych do sumy prawidłowych wyników pozytywnych oraz błędnych wyników pozytywnych, który można rozumieć jako zdolność modelu do niepoprawnej klasyfikacji próbek negatywnych jako pozytywne(patrz wzór 3),

$$\textbf{precision} = \frac{TP}{TP + FP} \tag{3}$$

- **miara *F*** - będąca średnią ważoną z czułości i precyzji(patrz wzór 4).

$$\textbf{F1} = \frac{2 * precision * recall}{precision + recall} \tag{4}$$

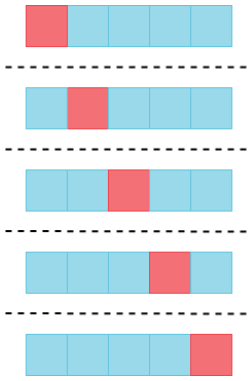
2.2.3 Krzywa ROC(*Receiver operating characteristic*)



Rysunek 4: Krzywa ROC

Krzywa obrazująca czułość i specyficzność przy różnych wartościach progu predykcji. Im większe pole pod krzywą tym lepszy klasyfikator. Na osi pionowej jest sensitivity a na poziomej specificity.

2.2.4 Walidacja krzyżowa/Sprawdzian krzyżowy



Rysunek 5: Krzywa ROC

Technika dokładnego testowania, Oryginalna próba jest dzielona na K podzbiorów. Następnie kolejno każdy z nich bierze się jako zbiór testowy, a pozostałe razem jako zbiór uczący i wykonuje analizę. Analiza jest więc wykonywana K razy. K rezultatów jest następnie uśrednianych (lub łączonych w inny sposób) w celu uzyskania jednego wyniku.

2.2.5 Techniki dostrajania i wyboru modelu

- **Wybór optymalnych hiperparametrów modelu** - Każdy model ma inne parametry do dostrajania, np. funkcje aktywacji w sieciach neuronowych czy głębokość drzew w lasach losowych. Nie ma standardowej procedury wyboru, najczęściej trenuje się model dla różnych wartości parametru i dobiera ten dla którego wyszedł najlepszy wynik. Grid search i random search, gradient descent itd.

- **Zmiana długości uczenia i wczesne zatrzymanie** - Przy zbyt długim uczeniu, może wystąpić efekt przeuczenia, czyli zbyt dokładnego dopasowania do danych treningowych, aby temu zapobiec, należy odpowiednio wcześnie zatrzymać uczenie, np. w momencie kiedy błąd na zbiorze walidacyjnym zaczyna rosnąć
- **Redukcja wymiarowości cech** W niektórych przypadkach zmniejszenie liczby cech może polepszyć działanie modelu, poprzez zapobieganie przeuczaniu i poprawę zdolności do uogólniania

2.3 Wykorzystanie głębokich sieci neuronowych do zadania klasyfikacji obrazów

2.3.1 Informacje Ogólne

W ostatnich latach nastąpił dynamiczny rozwój głębokich sieci neuronowych – dużych modeli, które wyewoluowały z klasycznych sieci neuronowych. Algorytmy uzyskują bardzo wysokie wyniki w wielu zadaniach takich jak: rozpoznawanie obrazu, rozpoznawanie mowy, analiza tekstu pisanego, synteza mowy. Zaletą głębokich sieci neuronowych do zadania klasyfikacji obrazów jest możliwość automatycznej ekstrakcji cech, w przeciwieństwie do klasycznych algorytmów rozpoznawania obrazu, których dobór wymaga wiedzy eksperckiej bazującej na tzw. inżynierii cech. Dzięki tej umiejętności, głębokie sieci neuronowe są w stanie wyodrębnić z badanego obrazu istotne cechy, które mają największy wpływ na możliwości klasyfikacji.

2.3.2 Konwolucyjne sieci neuronowe

Odmianą głębokich sieci neuronowych służącą do analizy obrazu są splotowe (konwolucyjne) sieci neuronowe. Typowa splotowa sieć neuronowa składa się z kombinacji 3 podstawowych typów warstw:

- warstwa splotowa(konwolucyjna),
- warstwa redukująca rozmiar (pooling).

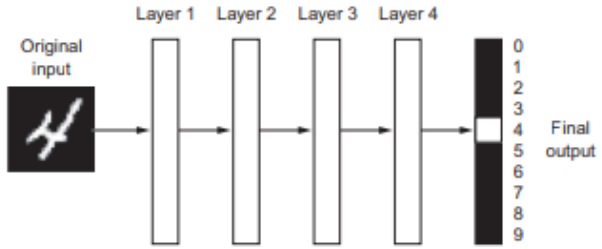
Dodatkowo wykorzystuję się klasyczne warstwy neuronowe tzw. warstwy pełnego połączenia. Splotowa sieć neuronowa przyjmuje na wejście obraz, który następnie jest przetwarzany przez kolejne warstwy. Warstwa splotowa wykonuje wielokrotnie operację splotu dyskretnego na obrazie wejściowym tworząc na wyjściu mapy cech. Operacja splotu dyskretnego w obszarach analizy obrazu wykorzystywana jest do filtracji. Następnie, przefiltrowane obrazy trafiają na nieliniową funkcję aktywacji, która przetwarza każdy piksel. Dodatkowo, po niektórych warstwach aktywacji umieszczona jest warstwa redukująca rozmiar, która zmniejsza liczbę pikseli w przetwarzanych obrazach. Wyjście ostatniej warstwy splotowej trafia na klasyczną sieć neuronową.

Uczenie klasycznych sieci neuronowych z dużą liczbą warstw jest bardzo trudne, często niemożliwe. W głębokich sieciach neuronowych wprowadzono szereg modyfikacji, które umożliwiły efektywny trening tak dużych modeli. Warstwy splotowe można interpretować jako zbiór neuronów połączonych z niewielką ilością neuronów w warstwie poprzedzającej, w przeciwieństwie do warstw klasycznych gdzie neuron połączony jest ze wszystkimi neuronami w poprzedniej warstwie. Ponadto, neurony posiadają grupowo współdzielone wagi (w ramach jednego filtru splotowego). Wymienione właściwości umożliwiają znaczną redukcję ilości parametrów, co umożliwia skuteczne uczenie takich struktur. Ponadto, szeroko stosowana funkcja aktywacji ReLU redukuje problem znikającego gradientu, ze względu na niemożliwość nasycenia się funkcji, jak ma to miejsce w klasycznych funkcjach aktywacji (funkcja sigmoidalna czy tangens hiperboliczny).

Cechą odróżniającą głębokie sieci neuronowe od klasycznych systemów klasyfikacji obrazów jest możliwość automatycznej ekstrakcji cech. Poprawna ekstrakcja cech jest kluczowym elementem każdego systemu klasyfikacji. Warstwy splotowe działają jako ekstraktor cech, które następnie podawane są na klasyczny klasyfikator neuronowy. W przypadku klasycznych systemów algorytmy ekstrakcji cech i ich parametry dobierane są przez badacza.

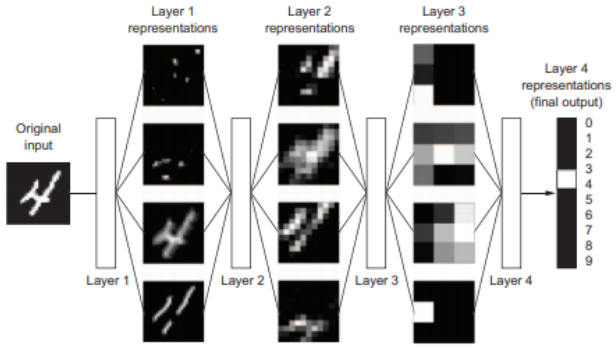
2.3.3 Przykład

- Klasyczna sieć neuronowa rozpoznająca cyfry:



Rysunek 6: Krzywa ROC

- Głęboka sieć konwolucyjna rozpoznająca cyfry:



Rysunek 7: Krzywa ROC

2.3.4 Przykładowe architektury

- LeNet(1990)
- AlexNet(2012)
- VGGNet(2014)
- ResNet(2015)

2.4 Metody redukcji wielowymiarowości

Redukcja wymiaru często jest pośrednim etapem w zagadnieniu klasyfikacji, analizy skupień czy regresji. W określonych sytuacjach pozwala na poprawę skuteczności tych metod, zwiększa stabilność a czasem pozwala na uwzględnienie w analizach dużej liczby zmiennych. Jest też popularnie wykorzystywaną metodą do wizualizacji wielowymiarowych zmiennych, dane są redukowane do przestrzeni dwuwymiarowej, w której już łatwo je przedstawić na wykresie. Metody z tej grupy są również nazywane metodami ekstrakcji cech, ponieważ w wyniku redukcji wymiaru tworzone są nowe cechy, które mogą być wykorzystane do innych zagadnień.

Jest to proces przekształcający pierwotny zbiór danych w zbiór o mniejszej liczbie wymiarów przy zachowaniu wszystkich lub większości informacji, które te dane ze sobą niosą. Wyróżnia się dwa główne typy redukcji wymiarowości:

- Selekcja atrybutów - redukcja zbioru uczącego do podzbioru składającego się tylko z najważniejszych atrybutów wykonuje się to poprzez takie operacje jak:
  - odrzucenie cech będących nadmiernie skorelowanych ze sobą
  - odrzucenie cech nieistotnych statystycznie
  - odrzucenie cech, które nie poprawiają wyników modelu
- Ekstrakcja atrybutów - łączenie atrybutów przy pomocy operacji liniowych bądź nieliniowych i tworzenie z nich nowych atrybutów łączących cechy wspólne.

2.4.1 Przekleństwo wielowymiarowości

Przekleństwo wymiarowości dotyczy problemu wykładniczego wzrostu danych w problemach związanych z uczeniem maszynowym. Oznacza to, że im większy wymiar tym znacznie więcej danych potrzebujemy. Dodatkowo oprócz potrzeby coraz większej ilości danych, to wykładniczo rośnie liczba możliwych wariantów, co znacznie zwiększa złożoność obliczeniową wykorzystywanych algorytmów. Rośnie również ryzyko przeuczenia a co za tym idzie spadku zdolności uogólniających klasyfikatora.

2.4.2 Zastosowania

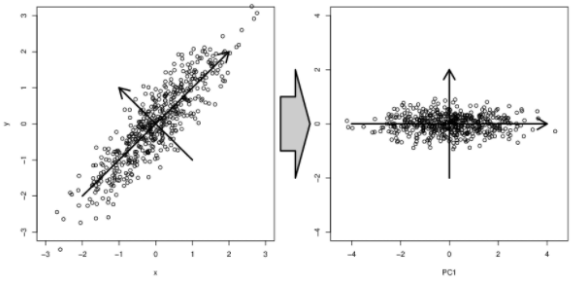
Istnieje wiele zastosowań redukcji wymiarów danych niektóre z nich to:

- **Możliwość wizualizacji oraz zrozumienia danych** - Ponieważ ludzki mózg bardzo dobrze odnajduje się w trójwymiarowej rzeczywistości przedmioty wykraczające ponad 3 wymiary są niemal niemożliwe do wyobrażenia. Aby rozwiązać ten problem można "spłaszczyć" dane do mniejszej liczby wymiarów a następnie zwizualizować je na przykład na wykresie.
- **Kompresja danych a co za tym idzie przyśpieszenie wykonywanych na nich obliczeń** - Redukcja wymiarów powoduje ogromne zmniejszenie się ilości danych do przeanalizowania. Pozwala to na przyśpieszenie szybkości uczenia algorytmów uczenia maszynowego.
- **Wykrywanie anomalii** – Zredukowanie wymiarów danych może często pozwolić na wyłapanie w prosty sposób danych niepasujących do zbioru, które mogą oznaczać anomalię lub niepoprawne dane.
- **Możliwość uniknięcia lub ograniczenia wpływu „przekleństwa wielowymiarowości"** - Zmniejszając ilość wymiarów analizowanych danych można zmniejszyć problem wykładniczej złożoności obliczeniowej algorytmów wykonywanych na nich.

2.4.3 Najczęściej wykorzystywane metody

- **Analiza składowych głównych** (ang. *Principal Components Analysis*)
  Analiza składowych głównych służy do wyznaczania nowych zmiennych, których możliwie mały podzbiór będzie mówił możliwie dużo o całej zmienności w zbiorze danych. Nowy zbiór zmiennych będzie tworzył bazę ortogonalną w przestrzeni cech. Zmienne będą wybierane w ten sposób by pierwsza zmienna odwzorowywała możliwie dużo zmienności w danych (po zrzutowaniu obserwacji na ten wektor, chcemy by wariancja rzutów była najwyższa). Po wyznaczeniu pierwszej zmiennej wyznaczamy drugą, tak by była ortogonalna do pierwszej, i wyjaśniała możliwie dużo pozostałej zmienności, kolejną zmienną wybieramy tak by była ortogonalna do dwóch pierwszych itd.

  Tak uzyskany zbiór wektorów tworzy bazę ortogonalną w przestrzeni cech, a co więcej pierwsze współrzędne wyjaśniają większość zmienności w obserwacjach. Celem metody składowych głównych jest więc znalezienie transformacji układu współrzędnych, która lepiej opisze zmienność pomiędzy obserwacjami. Przykład takiej transformacji rys 1. Przedstawiamy obserwacje w oryginalnym układzie współrzędnych (lewy rysunek) i w nowym układzie współrzędnych (prawy rysunek).



Rysunek 8: Przykład PCA

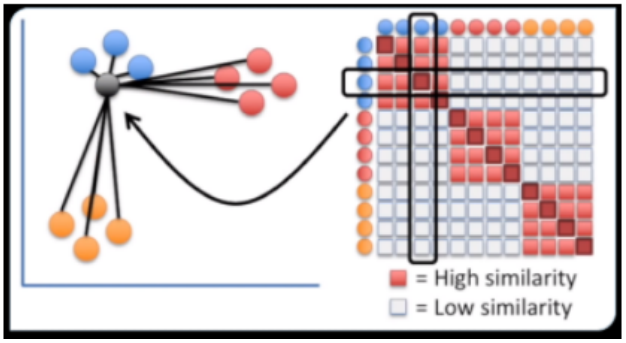
- **ISOMAP**
  ISOMAP jest metodą, która w porównaniu do pozostałych zdecydowanie lepiej radzi sobie z nieliniowymi danymi. Jej celem jest znalezienie niskowymiarowej reprezentacji danych, w której odległości rzeczywiste między elementami z próby są jak najbliższe tym z oryginalnej przestrzeni wysokowymiarowej.

  Kroki metody ISOMAP wyglądają następująco:
  - Wyszukiwanie najbliższego sąsiada - tworzony jest graf sąsiedztwa pomiędzy punktami w danych według zasady: jeżeli odległość między punktami jest mniejsza niż założona z góry odległość to tworzona jest krawędź pomiędzy tymi punktami.
  - Wyszukiwanie najkrótszej drogi – dla każdej pary punktów znajdowana jest najkrótsza odległość pomiędzy tymi punktami na utworzonym w kroku pierwszym grafie.
  - Skalowanie – stosowana jest metoda skalowania wielowymiarowego czyli technika przyjmująca na wejściu macierz odległości lub podobieństwa a następnie dąży do rozmieszczenia obiektów jako punktów w przestrzeni n-wymiarowej tak aby obiekty podobne do siebie znajdowały się bliżej. Wynikiem tego etapu jest reprezentacja danych w mniejszym wymiarze
- **T-SNE**
  T-SNE czyli stochastyczna metoda porządkowania sąsiadów w oparciu o rozkład t w porów-

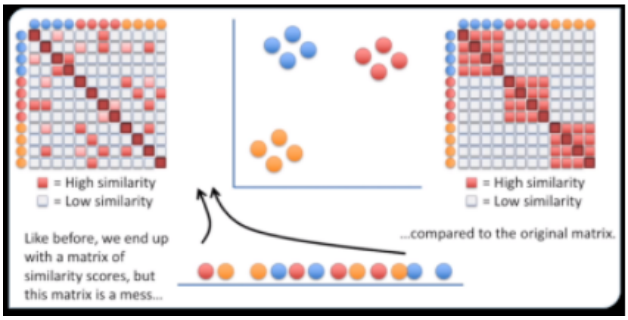
naniu do PCA jest ona droga obliczeniowo i dla dużej ilości wymiarów jej wyliczenie może zająć nawet kilka godzin gdzie PCA zakończy się w ciągu kilku minut. Jest ona także techniką probabilistyczną przez co nawet dla dokładnie tych samych parametrów jej obliczenie wiele razy da za każdym razem inny wynik.

Kroki tej metody wyglądają następująco:

– Wyliczenie podobieństw wszystkich danych



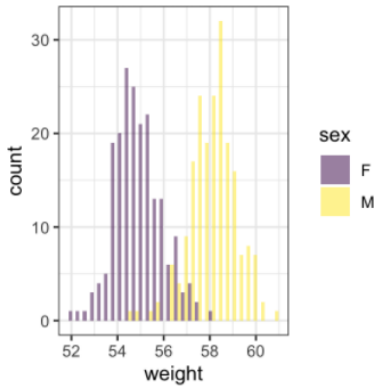
– Wyliczenie losowych podobieństw
– Odzwierciedlanie zestawów prawdopodobieństw w docelowej ilości wymiarów



2.5 Techniki prezentacji danych w aplikacjach webowych

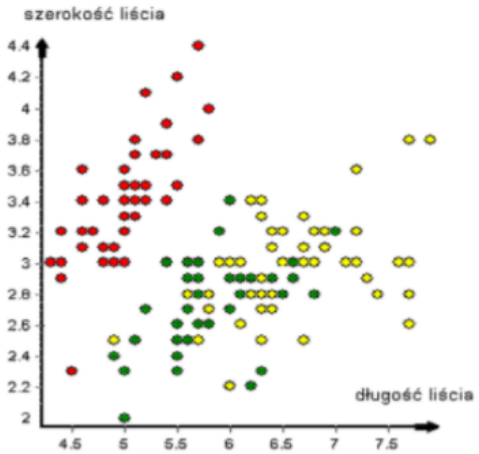
2.5.1 Wykresy jednej zmiennej

Są to metody, które pozwalają na wizualizację jednej cechy (dwóch licząc uwzględnienie klasy na wykresie np. przez kolor). Dzięki nim możemy obejrzeć rozkład cechy, wartości średnie, odchylenie standardowe itp.. Zaliczamy do nich m.in. wykresy pudełkowe oraz histogramy. Histogramy są narzędziem, dzięki któremu możemy graficznie odtworzyć rozkład danej cechy. Poza tym pozwalają one również dostrzec rozpiętość, skośność oraz szum danych. Często podczas tworzenia histogramów wprowadza się podział na klasy.

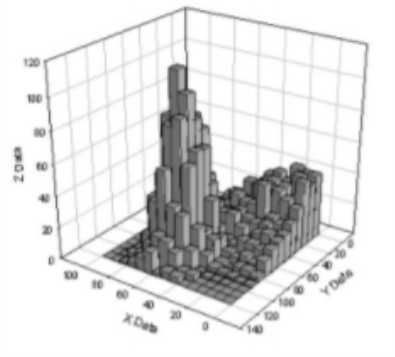


2.5.2 Rzut na dwie współrzędne

Do tej grupy zaliczamy metody, które pozwalają pokazać jednocześnie dwie współrzędne. Techniki te umożliwiają odkrycie związków między cechami (np. korelacja). Wykresy rozproszone (ang. scatterplot) są podstawowym narzędziem, które rzutuje dane na dwie współrzędne. Ich analiza powinna odbywać się pod kątem odkrycia korelacji między poszczególnymi cechami oraz klasteryzacji danych. Wykresy rozproszone są tworzone poprzez zaznaczanie kolejnych punktów danych w przestrzeni dwuwymiarowej. Wartość współrzędnej X odnosi się do pierwszej cechy, a Y do drugiej. Często mamy do czynienia z danymi podzielonymi na klasy



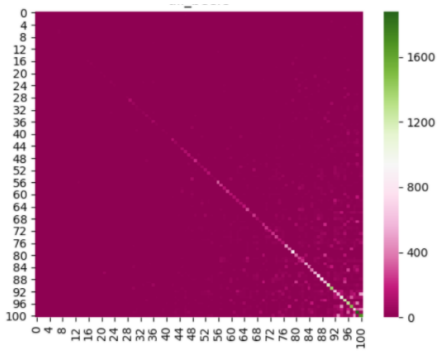
Drugą metodą pozwalającą jednoczesne pokazanie dwóch cech są, wcześniej wymienione, histogramy dwuwymiarowe



2.5.3 Metody używające koloru i odcieni

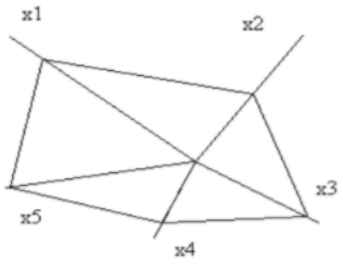
Jest to kolejny pomysł na wizualizację danych, wykorzystujący naturalne ludzkie zdolności rozróżniania kolorów (dotyczy ludzi nie cierpiących na choroby takie jak daltonizm). Do metod tych należą prostokąty heatmap'y, gdzie kolor odpowiada wartości cechy w zależności od dwóch pozostałych współrzędnych.

Heatmap'y są także wykorzystywane przy dużych zbiorach danych, np. do macierzy konfuzji przy sprawdzaniu modeli sztucznej inteligencji. Bardziej niż na dokładnej wartości, zależy nam aby sprawdzić czy przewidywane klasy odpowiadają rzeczywistym, i na pierwszy rzut oka da się dostrzeć w jakich obszarach/jakie klasy błędnie interpretuje np. sieć neuronowa



2.5.4 Metody korzystające z osi gwiazdowych (radarowych)

Ta grupa składa się tylko z jednej metody czyli wykresów gwiazdowych (ang. star plot, radar plot). Technika pozwala na zaprezentowanie danych wielowymiarowych z dowolną ilością zmiennych. Każdy wektor cech jest reprezentowany przez wykres, przypominający gwiazdę, w którym każdy promień przedstawia jedną zmienną


x1
x2
x3
x5
x4

2.6 Definicje, charakterystyka i zastosowania rzeczywistości rozszerzonej i wirtualnej

2.6.1 Rzeczywistość rozszerzona(*Augmented reality*)

System łączący świat rzeczywisty, realny, oraz rzeczywistość wirtualna. Taki system jest interaktywny w czasie rzeczywistym, umożliwia on swobodę ruchów w trzech wymiarach. W celu wytworzenia rzeczywistości rozszerzonej zwykle jest potrzebny aparat, ekran na którym będzie wyświetlana informacja oraz generowana w czasie rzeczywistym grafika 3D lub 2D. AR można podzielić na trzy rodzaje:

- AR bazujący się na znaczniku lub znacznikach
- AR który nie używa znaczników
- AR bazujący się na lokalizacji.

Pierwszy rodzaj AR używa tak zwane znaczniki. Znacznik to obraz lub obiekt który śluzy elementem wskazującym na miejsce gdzie musi być umieszczony trójwymiarowy object, jego rozmiar i położenie. Plusem wykorzystania znaczników można nazwać wysoką precyzje położenia wygenerowanych obiektów 3D lub 2D. Minusem znaczników można nazwać to że gdy on zostanie zgubiony, cała scena AR znika.

AR który nie używa znaczników zazwyczaj skanuje otoczenia za pomocą kamery w celu wykrycia płaskiej powierzchni, na której potem będzie umieszczony object 3D. Zaletą takiego typu AR jest to że gdy taka powierzchnia zostanie rozpoznana, użytkownik może nie straszyć stracenia znacznika AR i może łatwiej poruszać wokół zeskanowanej powierzchni. Jednak za taką swobodę użytkownik płaci czasem potrzebnym na zeskanowanie tej powierzchni.

Trzeci rodzaj AR bazuje się na lokalizacji. Scena AR zostanie uruchomiona w odpowiednim miejscu, dla którego ona została zaprojektowana.

Istnieje wiele różnych rodzajów urządzeń za pomocą których AR może być wyświetlany, między innymi to:

- Handheld AR (do tego można odnieść smartphone i tablet),
- Smart glasses (optyczne okulary, czyli takie w których używane przezroczyste lub pół przezroczyste powierzchnie do wyświetlania grafiki 3D lub 2D, Microsoft's Hololens, Magic Leap One, Google Glass. Okulary VR posiadające zintegrowane aparaty, w takich okularach na ekran lub ekrany przekazywany jest widok otoczenia z aparatów oraz wygenerowane grafiki 3D lub 2D, HTC Vive VR)
- HUD - Head-Up Display (przezroczysta lub pół przezroczysta powierzchnia na którą wyświetlana jest projekcja, projektor lub ekran który przekazuje informacje na powierzchnię oraz komputer generujący obrazy do wyświetlania)
- Ekrany montowane na kasku (działa podobnie do HUD)
- Ekrany holograficzne (Istnieje wiele różnych rodzajów takich typów ekranów, prostym przykładem jest stworzenie tak zwanej piramidy, umieszczenia szkła pod kątem 45 stopni)

2.6.2 Zastosowanie AR

- AR w przemyśle
  Używanie okularów AR dla wspomagania pracownika w celu wytwarzania jakiegoś produktu lub sprawdzenia jakości jego wytworzenia (zastosowanie Google Glass na fabrykach Boeing,

BIManywhere i TrimbleConnect dla budownictwa — pozwala pokazać rury i kable które muszą być zainstalowane w budynku, sprawdzenie czy wszystko zostało zrealizowane zgodnie z projektem)

- AR w medycynie:
  Demonstracja różnych chorób dla pacjenta czy dla uczenia uczniów i lekarzy (Demonstracji anatomii dla uczniów, demonstracji skutków choroby dla pacjenta — jeżeli pacjent ma chore wzroku , można jemu zademonstrować skutki nie leczenia tej choroby)
- AR dla wojska:
  Informowanie żołnierzy o swoim otoczeniu, informacja dla pilota

2.6.3 Rzeczywistość wirtualna (*virtual reality*)

Komputerowo wygenerowany trójwymiarowy obraz, który imituje świat realny lub stanowi wizję świata fikcyjnego. W takie wygenerowane przez komputer otoczenie osoba może całkowicie się zanurzyć. Taki system tak samo jest systemem interaktywnym i umożliwia ruch w trzech wymiarach za pomocą dedykowanych sensorów lub kamer. W celu umieszczenia osoby w rzeczywistości wirtualnej zwykle jest potrzebny ekran lub dwa ekrany, specjalne soczewki oraz komputer generujący ten wirtualny świat. Okulary VR mogą być dwóch rodzajów: wyposażone lub nie wyposażone w specjalny mini komputer generujący ten świat.

Przykładem zwykłych okularów VR są Oculus Rift, HTC Vive i inne. Oculus Quest z innej strony zawiera w sobie płytę główną, procesor i baterie dla pracy autonomicznej, bez podłączania do komputera. Istnieje również możliwość umieszczenia smartfona w dedykowanych okularach. Interakcja z takim wirtualnym światem może odbywać za pomocą zwykłego kontrolera lub nawet klawiatury i myszy.

Zaawansowane systemy VR wyposażone w specjalne kontrolery ułatwiające sterowanie otoczeniem.

Systemy VR również mogą zawierać sensory które mapują położenie użytkownika w świecie fizycznym przenosząc dane o jego położeniu do świata wirtualnego. Takie sensory najczęściej umieszczane na suficie aby pokrywać dużą powierzchnie. Dodatkowo można umieścić sensory na czele użytkownika aby lepiej przenieść jego ruch do świata wirtualnego

2.6.4 Zastosowanie VR

- **Diagnozowanie i leczenie chorób** związanych z zdrowiem psychologicznym np. rehabilitacja osób z Alzheimerem
- Używanie **VR jako terapii** (Za pomocą VR lekarzy mogą wizualizować halucynacji dla osób chorych na Schizofrenię co pomaga walczyć z nimi, też jest możliwe przeprowadzenie terapii przeciwbólowej)
- **Trenowanie i uczenie** (na przykład trenowanie lekarzy dla przeprowadzenia skomplikowanych operacji, trenowanie wojskowych)

2.7 Charakterystyka wybranych zjawisk i procesów w kontekście ich symulacji komputerowej

Symulacja w świecie cyfrowym to kopiowanie działania jakiegoś systemu lub jego części. Precyzyjniej „symulację komputerową" można nazwać sposobem numerycznym stosowanym do przeprowadzania eksperymentów na konkretnych typach modeli matematycznych, które charakteryzują się użyciem maszyny cyfrowej pracę złożonego systemu w dłuższym okresie. Symulacje spotykamy w naszym życiu codziennym I nie zwracamy już na nie uwagi. Oczywistym przykładem są prognozy pogody, w których to, dzięki tysiącom, a nie rzadko milionom obliczeń symulujemy zachowania pogody, w konsekwencji czego czerpiemy z nich istotne dla nas informacje, tj. Przewidywaną temperaturę czy też pojawienie się niekorzystnego zjawiska atmosferycznego. Symulacja służy nam również do badania procesów, których nie możemy wykonać „na żywo" przykładami są tutaj testy różnych reakcji jądrowych, czy też zachowanie się różnych ciał niebieskich przy różnych współczynnikach je kształtujących. Symulacje stały się nieodzownym elementem badań I ich przebieg jest często bardzo zbliżony:

- Wytyczenie problemu,
- Wytworzenie modelu matematycznego,
- Ustalenie programu dla komputera,
- Kontrola bezbłędności systemu,
- Zorganizowanie badań symulacyjnych,
- Przeprowadzenie przebiegu symulacji i weryfikacja wyników.

Symulacje komputerowe dzielą się pod kątem:

- **Przewidywalności wydarzeń**
  - **stochastyczne** - używają generatora liczb pseudolosowych czy czasem losowych (najbardziej znana metoda to Monte Carlo),
  - **deterministyczne** (wynik powtarza się i uzależniony jest jedynie od danych wejściowych, jak i kontaktów ze światem zewnętrznym.
- **Metody upływu czasu**
  - **Z czasem ciągłym** - czas rośnie ciągłymi przyrostami, a krok czasowy wybiera się optymalnie z powodu żasobożernościśystemu, jego sprawności i postaci,
  - **Symulacja zdarzeń dyskretnych** - czas rośnie stopniowo, lecz jego przyrosty są różne.
- **Stylu danych wejściowych**
  - **Statyczne** - efekt to zbiór danych,
  - **Dynamiczne** - efekt to proces odbywający się w czasie np. animacja,
  - **Interaktywne** - działają poprzez sygnały z zewnątrz.
- **Ilości zastosowanych komputerów**
  - **lokalne** - do przetworzenia służy komputer,
  - **rozproszone** - do przetworzenia służy wiele komputerów.
- **Programowania agentowego** - jest to specjalna forma symulacji dyskretnych, nieopierających się na danym modelu, lecz możliwa do przedstawienia.

Symulacja komputerowa znalazła również swoje zastosowania w świecie finansów. Banki dzięki zbieraniu danych historycznych oraz biorąc pod uwagę aktualne czynniki gospodarcze, szybko są w stanie wykreować nasz profil inwestora, czy też klienta. Niewątpliwie symulacje giełdowe cieszą się największym zainteresowaniem I nad nimi są prowadzone największe badania w tym sektorze, ponieważ potencjalne zyski jakie mogą przyjść wraz z symulowaniem przyszłości są ogromne. Niestety symulowanie układów otwartych jakim jest nasz świat jest niezwykle ciężkie I zasobożerne, dlatego nie mamy jeszcze komputerów, które przewidują ze sporą dokładnością wahania rynkowe.

Zwyczajnie czynników, które wpływają na owe wahania jest zbyt wiele. Warto znów tutaj wrócić, do prognoz pogody, które jak sami widzimy najczęściej sprawdzają się jedynie dzień wprzód, zaś każdy następny dzień zmniejsza prawdopodobieństwa prawdziwego przewidzenia pogody.

Symulacje znalazły zastosowanie również w świecie rozrywkowym I to nimi właśnie zajmowaliśmy się głównie na kursie Analiza I Symulacje w zeszłym roku. Tutaj skupiamy się głównie na symulacjach ruchu. Na wykładzie przedstawiono nam 3 rodzaje animowania ruchu:

- określanie gdzie ma się co znaleźć w danej chwili,
- motion capture,
- symulowanie na procesorze/karcie graficznej.

W pierwszym podejściu musimy jasno pokazywać gdzie dany obiekt musi się znaleźć w kolejnych momentach trwania animacji, a tranzycję (przejścia) pomiędzy wytyczonymi punktami można przeprowadzić, posiłkując się metodami interpolacji (kilka omówiliśmy na wykładzie). Problemem jest tutaj jednak dobór kroku czasowego, aby zachować odpowiednią dynamikę ruchu – tutaj najczęściej posługujemy się całkami, aby wyznaczyć przybliżone tory ruchu.

Drugą metodą przeniesienia ruchu do komputera są systemy motion capture. Ta technika, pomimo że się wydaje najdokładniejsza, ponieważ od razu rozwiązuje problem płynnych przejść pomiędzy scenami, to ma swoje wady. Największą wadą jest to, że kolejne elementy kostiumu motion capture muszą być przyczepione do bohatera, a nie do jego odzieże, w konsekwencji możemy mówić, że animacje skąpo ubranych bohaterów będą dobre I zbliżone do rzeczywistości, jednak już osoba ubrana w długi płaszcz będzie wyglądać nienaturalnie, ponieważ dodanie płaszcza jest sztuczne I pomimo, iż wydaje się to błachostką symulacja zachowania płaszcza w reakcji na poszczególne ruchy swojego właściciela jest czasami nienaturalna, szczególnie widoczne jest to w świecie gier komputerowych.

Ostatnim podejściem do animacji to zrzucenie wszystkiego na barki procesora i – jeśli to możliwe – opisanie jakiegoś procesu modelem fizycznym i numeryczne rozwiązywanie go. Podejście dobre lecz wymaga optymalizacji tz. Jak dokładna ma być nasza symulacja.

Można jeszcze dopowiedzieć o metodach numerycznych wykorzystywanych do uproszczenia równać ruchów, czy też ich znajdowania w ogóle. Całkowanie numeryczne metody:

- prostokątów - najprostrza I najmniej zasobożerna, ale nie najlepsza
- trapezów – ta już dokładniej przybliży krzywe całki I chyba jest najczęściej wykorzystywana
- parabol Simsona

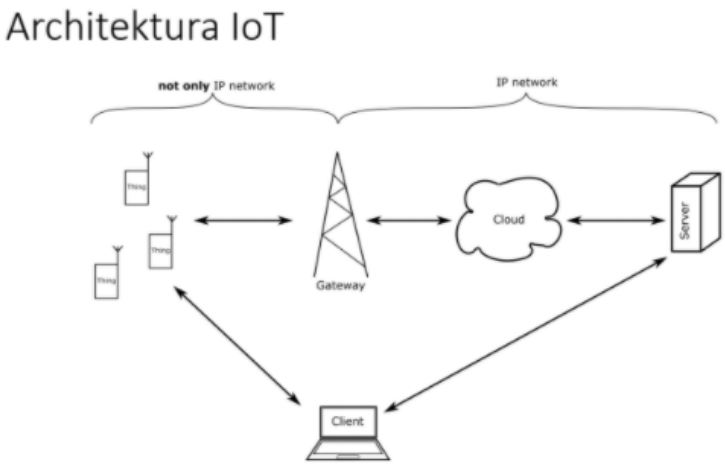
2.8 Wyzwania i metody zapewniania bezpieczeństwa systemów autonomicznych i sieci IoT

2.8.1 Wyzwania IoT

- Trudne zapewnienie fizycznej ochrony sprzetu,
- Bezpieczeństwo danych wysłanych przez urządzenia i przechowywanych w chmurze
- Domyślne hasła urządzeń,
- Domyślny brak filtrowania ruchu,
- Brak zasobów do implementacji silnych zabezpieczeń,
- Zapewnienie bezpiecznego połączenia urządzenia z chmurą obliczeniową

2.8.2 Mechanizmy bezpieczeństwa sieci IoT

- Identyfikacja (np. Po IMEI urządzenia) i autentykacja wszystkich urządzeń w sieci w celu ochrony przed podszywaniem się pod urządzenia,
- kontrola dostępu pomiędzy urządzeniami:
  - wykorzystywanie VPN, tunelowania L2TP (protokół tunelowania warstwy drugiej) lub IPsec,
  - Konfiguracja dostępu do zasobów w oparciu o konkteks działania – limitowanie dostępu tylko do potrzebnych informacji
- szyfrowanie przesyłanych danych
- utrzymanie dostępności zasobów:
  - implementacja przetestowanych, certyfikowanych i ustandaryzowanych technologi komunikacji, np. GSM, UMTS, LTE,
  - Technologie radiowe IoT:
  - konfiguracja odpornych na przeciążenia i ataki topografii sieci,
  - monitorowanie na żywo 24/7 zasobów sieci i wydajności urządzeń
  - Niezawodność transmisji
    - nadmiarowość
    - wykrywanie błędów
      - ACK
      - żądania retransmisji
    - korygowanie błędów
- testy bezpieczeństwa kodu źródłowego urządzeń IoT (wycieki pamięci, przepełnienie bufora)
- zapewnienie aktualizacji bezpieczeństwa wykorzystywanego oprogramowania
- unikanie inicjacji połączenia przez urządzenia – jedynie przez firewalle, proxy lub listy dostępu w celu ograniczenia ryzyka ataku na systemu wewnętrzne
- oddzielenie sieci urządzeń od sieci serwerów współdzieloną, zabezpieczoną firewallem siecią przekazywania danych



Rysunek 9: Krzywa ROC

2.8.3 System autonomiczny - wyzwania

- prawa jednostki vs. prawa ogółu
- Social Credit System w Chinach
- prawa robotów (sztucznej inteligencji)
- prawo karne
- egzekwowanie
- zapobieganie
- prawo pracy
- prawo własności intelektualnej
- etyka
- ogromna ilość danych
- komunikacja
- przetwarzanie
- przechowywanie
- bezpieczeństwo
- zarządzanie infrastrukturą
- koszt energetyczny
- koszt

2.8.4 Wyzwania technologiczne

- gromadzenie danych
  - sensory
  - sieci komunikacyjne
  - przechowywanie
- przetwarzanie danych
  - dostępność
  - algorytmy
- autonomiczność pracy
  - zasilanie
  - niezawodność

2.9 Przetwarzanie i gromadzenie informacji w systemach rozproszonych, autonomicznych i sieciach IoT

Architektury, warstwy" wykorzystywane w przetwarzaniu danych w takich systemach to:

- **Cloud** (chmury obliczeniowe)
- **Fog** (mgła obliczeniowa)
- **Edge** (urządzenia brzegowe)
- **Mist** (sensor/ end-node)

2.9.1 Cloud

Zazwyczaj urządzenia IoT mają małą moc obliczeniową i niewielką ilość pamięci, z tego powodu rozwiązania chmurowe są bardzo popularne, ponieważ zapewniają skalowalne zasoby do przetwarzania i przechowywania danych na żądanie. Dane z sensorów są transportowane do centrum obliczeniowego, gdzie są przetwarzane, a wynik jest przesyłany do zasubskrybowanych aplikacji. Ponadto centra obliczeniowe mogą przechowywać dane w celu analizy i wydobycia z nich wiedzy.

Zalety chmury obliczeniowej to:

- brak konieczności utrzymywania własnej infrastruktury obliczeniowej.
- możliwość szybkiej realizacji projektów i testowania koncepcji bez dużych zakupów IT i dużych kosztów początkowych (płaci się tylko za zużyte zasoby).
- jeżeli dane wysyłane/odczytywane są rzadko to wykorzystanie rozwiązań chmurowych jest tańsze, bo nie trzeba pozostawiać w stanie bezczynności dedykowanego sprzętu i oprogramowania.
- duża wydajność, elastyczność, skalowalność
- niezawodność przy założeniu stabilnego połączenia
- łatwość w wykorzystaniu tych samych danych przez wiele grup/aplikacji

Jednak ta technologia ma swoje wady np:

- wymaga stałego dostępu do Internetu, często o dużej przepustowości
- niektóre przedsiębiorstwa mogą być niechętne umieszczaniu krytycznych danych w chmurze z powodu obawy o bezpieczeństwo danych
- nie nadaje się do aplikacji, które potrzebują danych do analizy w czasie rzeczywistym, ponieważ trzeba wysłać dane z węzła aż do chmury co generuje opóźnienia

2.9.2 Fog

W mgle obliczeniowej przetwarzanie danych odbywa się na urządzeniach, które znajdują się na krawędzi sieci. Do urządzeń brzegowych należą routery, switche, access pointy wifi, set-top-boksy, stacje bazowe itd. Urządzenia te nie są już używane wyłącznie do przesyłania danych, lecz posiadają

znaczne możliwości obliczeniowe oraz pamięć masową.

Zadania obliczeniowe, które w przeciwnym razie musiałby zostać przesłane do jakiejś chmury mogą zostać zrealizowane lokalnie, minimalizuje to czas przetwarzania, a co jest szczególnie ważne dla aplikacji, które muszą działać w czasie rzeczywistym.

Architektura mgły obliczeniowa może być scentralizowana lub rozproszona lub być kombinacją obu. W architekturze scentralizowanej każdy węzeł działa pod węzłem centralnym, zarządzanie taką siecią jest łatwe, ale gdy liczba podłączonych urządzeń wzrasta to staje się to wyzwaniem. W rozproszonej architekturze urządzenia współdziałają w sposób peer-to-peer.. Obciążenia obliczeniowe są rozproszone pomiędzy urządzeniami,. Każdy z węzłów mgły komunikuje się z innymi np. w celu podziału pracy.

Można wyróżnić 3 rodzaje komunikacji:
- **Machine-to-machine** - dane generowane przez jedno urząđzenie są konsumowane przez inne urządzenia
- **machine-to-people** - dane generowane przez urządzenia są konsumowane przez ludzi i i vice versa
- **people-to-people** - dane generowane przez ludzi są konsumowane przez ludzi

Czas trwania tych interakcji może wynosić od sekund do dni. Na przykład, interakcja w aplikacjach działających w czasie rzeczywistym trwa od kilku sekund do kilku minut. Natomiast analiza transakcyjna może trwać kilka dni.

Architektura Fog zmniejsza również obciążenie połączeń sieciowych, ponieważ większość komunikacji dzieje się w pobliżu użytkownika, więc bardzo niewiele łączy sieciowych jest zaangażowanych w dane/usługi we mgle mając na uwadze, że w przypadku architektury Cloud cała sieć może zaangażować się w świadczenie usługi do użytkownika końcowego.

Oprócz dostarczania usługi dla użytkowników końcowych może również zarządzać ruchem sieciowym, jak również w razie potrzeby może korzystać z zasobów chmury, gdy przetwarzanie danych przekracza jej możliwości.

Wady:
- magazynowanie danych,urządzenia nie mają odpowiedniej pojemności. do przechowywania dużych ilości danych przez bardzo długi czas ze względu na różne ograniczenia fizyczne.
- architektura ze względu na ograniczoną moc obliczeniową urządzeń IoT, co sprawia, że mgła nie nadaje się do użytku dla usług związanych z ciężkimi obliczeniami.

Globalna koordynacja: Architektura chmury wspiera globalną koordynację, ponieważ jest to scentralizowana architektura, w której chmura może nawet koordynować pomiędzy różnymi urządzeniami Fog w całym obszarze globu

2.9.3 Edge

Edge computing może być używany do przetwarzania danych bezpośrednio na urządzeniach, które mają dołączone czujniki lub urządzeń bramowych, które są blisko czujników. W związku z tym, obliczenia krawędziowe mogą umożliwić urządzeniom przetwarzanie danych bez polegania na

chmurze lub mgle. Przetwarzając dane bliżej krawędzi, obliczenia krawędziowe mogą umożliwić urządzeniom przetwarzanie danych w czasie zbliżonym do rzeczywistego. W związku z tym, obliczenia krawędziowe mogą zmniejszyć koszty ogólne w scentralizowanej chmurze.

Obliczenia krawędziowe mogą być wykorzystywane w podłączonych domach do wykonywania zadań, takich jak włączanie grzejnika lub oświetlenia w czasie zbliżonym do rzeczywistego.

2.9.4 Mist

Mist computing to ekstremalna wersja edge computingu, zwykle składa się z mikrokontrolerów i czujników. Umożliwienie zbierania danych poprzez zdolności obliczeniowe i komunikacyjne samego czujnika.

Obsługa komunikacji wymaga często większość mocy obliczeniowej mikrokontrolera, zbierając surowe dane i filtrując je jesteśmy w stanie wysyłać tylko istotne dane do stacji bazowej, routera czy też serwera, co umożliwia oszczędzanie energii i przepustowości.

Przetwarzanie danych na urządzeniu brzegowym obejmuje często takie rzeczy jak:
- Normalizacja lub przekształcenie danych do jednolitego formatu, zapewniając, że format ten jest zgodny z aplikacją.
- Dane "opakowaniowe" w sposób, który jest bezpieczny i łączy dane w "praktyczną partię".
- Walidacja danych w celu zapewnienia ich zgodności z szeregiem ustalonych reguł.
- Sortowanie danych w celu utworzenia preferowanej sekwencji
- "Podsumowywanie/kompresowanie danych" w celu zmniejszenia objętości i wyeliminowania niepotrzebnych lub niepożądanych szczegółów.
- Filtrowanie powtarzających się, nieaktualnych lub niepożądanych danych w celu zwiększenia ich dokładności.
- Wzbogacanie danych za pomocą dodatkowych powiązanych informacji (metadata)

2.10 Współczesne zagrożenia bezpieczeństwa oraz sposoby przeciwdziałania im

Pojęcie „zagrożenia" jest często błędnie używane - według standardów ISO 27000 i 27005 zagrożenia bezpieczeństwa (aby nie mylić z podatnościami lub ryzykiem) to zdarzenia które mają potencjał zagrażać bezpieczeństwu systemu (tzn. wpłynąć na poufność, integralność lub dostępność). [Podatności to słabości systemu które mogą zostać wykorzystane przez zagrożenia, np. zagrożenie: pożar, podatność: brak kopii zapasowej i to skutkuje ryzykiem utraty danych]

Zagrożenia są zawsze obecne, ale można im przeciwdziałać poprzez procedury bezpieczeństwa. Przez przeciwdziałanie rozumiane są działania mające na celu powstrzymanie negatywnego wpływu zagrożenia, lub jeżeli jest to niemożliwe, zredukowanie skutków lub ułatwienie czynności naprawczych.

Przeciwdziałanie zagrożeniom jest powiązane z pojęciem zarządzania ryzykiem, ponieważ akcje i procedury mające przeciwdziałać zagrożeniom są zazwyczaj tworzone mając na uwadze prawdopodobieństwo, że zagrożenie wykorzysta pewną podatność, oraz jak duży wpływ będzie to miało na bezpieczeństwo systemu. Tworząc plany przeciwdziałania trzeba też mieć na uwadze koszty oraz wpływ na jedną z części bezpieczeństwa – dostępność. Przeciwdziałanie zagrożeniom musi więc być opracowane dla konkretnego przypadku – nie ma sensu budować budynku odpornego na trzęsienia ziemi w Polsce, lub wydawać milionów na ochronę danych wartych kilkanaście tysięcy.

Istnieją dwa główne sposoby kategoryzacji zagrożeń zaproponowane przez standard ISO 27005:

- ze względu na **źródło pochodzenia** - wydarzenia naturalne (E - environmental), wydarzenia przypadkowe (A - accidental) i wydarzenia umyślne (D - deliberate)
- ze względu na **typ zagrożenia**: uszkodzenia fizyczne, klęski żywiołowe, utrata niezbędnych mediów, zakłócenia spowodowane promieniowaniem, utrata kontroli nad danymi, uszkodzenia techniczne, nieautoryzowane działania, niemożność zrealizowania czynności biznesowych. Sposoby przeciwdziałania zagrożeniom są zazwyczaj podobne dla różnych zagrożeń tego samego typu.

2.10.1 Przykłady zagrożeń i sposoby przeciwdziałania

- **Uszkodzenia fizyczne**
  - Pożar (A,D,E)
  - Zniszczenie sprzętu lub nośników danych (A,D,E)
  - Przeciwdziałanie:
    - geo-replikacja danych/usług, tak aby strata jednej lokacji nie wiązała się z utratą danych czy dostępności.
    - Przestrzeganie najnowszych zarządzeń p.poż
- **Klęski żywiołowe**
  - Powódź (E)
  - Trzęsienie ziemi (E)
  - Przeciwdziałanie:
    - Geo-replikacja
    - Odpowiedni dobór lokalizacji sprzętu/danych
- **Utrata niezbędnych mediów**
  - Utrata zasilania (A,D,E)
  - Utrata połączenia z Internetem (A,D)

  - Przeciwdziałanie:
    * Duplikacja mediów – np. internet od 2 dostawców, po innej infrastrukturze sieciowej, awaryjny generator prądu
- **Zakłócenia spowodowane promieniowaniem**
  - Zakłócenia spowodowane promieniowaniem elektromagnetycznym (A,D,E)
  - Zakłócenia spowodowane promieniowaniem cieplnym (A,D,E)
  - Przeciwdziałanie:
    * Ekranowanie wrażliwych elementów
    * Redundantne systemy głosujące nad decyzją
- **Utrata kontroli nad danymi**
  - Kradzież lub manipulacja sprzętu/dokumentów (D)
  - Phishing (D)
  - Wyciek danych (A,D)
  - Przeciwdziałanie:
    * Implementacja systemów kontroli dostępu
    * Szkolenie pracowników w zakresie bezpieczeństwa komputerowego, w szczególności Social Engineering
    * „Znaki wodne"
- **Uszkodzenia techniczne**
  - Błędne działanie sprzętu (A)
  - Przepełnienie systemów zbioru informacji (A,D)
  - Przeciwdziałanie:
    * Kupowanie i eksploatacja renomowanego sprzętu, o wysokiej odporności na uszkodzenia
    * Regularne/automatyczne przeglądy techniczne
- **Nieautoryzowane działania**
  - Nielegalne przetwarzanie danych (D)
  - Użycie podrobionego lub skopiowanego oprogramowania (A,D)
  - Przeciwdziałanie:
    * Szkolenie pracowników w zakresie praw przetwarzania danych oraz własności intelektualnej
    * Instalacja oprogramowania tylko przez profesjonalnych administratorów
- **Niemożność zrealizowania czynności biznesowych**
  - Brak dostępności personelu (A,D,E)
  - Błędne wykonanie procedur (A)
  - Przeciwdziałanie:
    * Zatrudnianie odpowiedniej ilości pracowników i nieskupianie wiedzy w pojedynczych jednostkach
    * Szkolenie pracowników

2.11 Klasyfikacja złośliwego oprogramowania. Definicja i kroki analizy powłamaniowej

Klasyfikacja złośliwego oprogramowania Szkodliwe oprogramowanie/malware - programy mające szkodliwy wpływ na system komputerowy/użytkownika Klasyfikacja:

- **Backdoor** - luka w zabezpieczeniach systemu utworzona umyślnie w celu późniejszego wykorzystania
- **Bomba logiczna**(*logic bomb*) - fragment kodu celowo wstawiony do systemu, uruchamiający złośliwą funkcję, gdy zostaną spełnione określone warunki, np. atak uruchamiany przez określone wydarzenie, datę lub godzinę
- **Botnet** - grupa komputerów (zombie) zainfekowanych szkodliwym oprogramowaniem (np. robakiem) pozostającym w ukryciu przed użytkownikiem i pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami w ramach botnetu; wykorzystywany m. in. do ataków DDoS
- **Exploit** - kod umożliwiający bezpośrednie włamanie do komputera ofiary wykorzystujący konkretne bugi lub słabości oprogramowania ofiary
- **Adware** - oprogramowanie, wyświetlające niepożądane przez odbiorcę reklamy.
- **Spyware** - gromadzi informacje o użytkownikach bez ich wiedzy
- **Ransomware** - blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego
- **Robak**(*worm*) - analogicznie do wirusów rozprzestrzeniają się poprzez sieć; w odróżnieniu od wirusów nie wymagają programu hostującego, zamiast tego wykorzystują luki w zabezpieczeniach systemów lub stosują socjotechniki, aby użytkownik je uruchomił
- **Koń trojański** - klasa zagrożeń komputerowych, które wydają się wykonywać pożądaną funkcję, ale w rzeczywistości wykonują niejawne złośliwe funkcje
- **Rootkit** - zaprojektowany w celu ukrycia lub zamaskowania faktu naruszenia bezpieczeństwa systemu, np. ukrywa istnienie szkodliwych procesów lub plików przed użytkownikiem
- **Keylogger** - odczytują i zapisują wszystkie naciśnięcia klawiszy użytkownika próbując wybrać wzorce, które synchronizują się z pewnymi informacjami
- **Wirus** - program lub fragment kodu, potrafiący się replikować i zainfekować komputer bez zgody lub wiedzy właściciela

2.11.1 Definicja i kroki analizy powłamaniowej

Analiza powłamaniowa - polega na gromadzeniu dowodów do postępowania sądowego lub po prostu analizie informacji, które pozwolą odtworzyć metodologię ataku zastosowaną przez cyberprzestępców

Kroki analizy powłamaniowej:

- **wykrycie włamania** - wszystko, co wygląda na nienormalne – nie dające się wytłumaczyć normalnym działaniem systemu bez ingerencji administratora, np. pliki w katalogach systemowych z datą modyfikacji (lub ctime) w przyszłości, ctime plików systemowych inny niż z daty instalacji/aktualizacji systemu, katalogi o podejrzanych nazwach jak "..." lub ".. " (dwie kropki i spacja), niewłaściwe prawa dostępu plików systemowych
- **szukanie śladów** - dla potwierdzenia włamania, wskazujących na sposób dokonania włamania (ślady exploitów lub innych luk), w celu oszacowania „strat" (zakresu włamania), w celu znalezienia potencjalnych furtek; szukać należy w logach systemowych, konfiguracji systemu,

przy użyciu komend diagnostycznych i/lub snapshotów konfiguracji (np. tripware)

- **przywrócenie stanu sprzed włamania** - unieszkodliwienie furtek, odtworzenie zmodyfikowanych plików i konfiguracji systemu
- **zabezpieczenie systemu na przyszłość** - instalacja łat oprogramowania, poprawienie konfiguracji systemu, zainstalowanie dodatkowych zabezpieczeń (firewalle itp.)

2.12 Zastosowania, zasady budowy i funkcjonowania cyfrowych asystentów

Najpierw trzeba przedstawić czym jest asystent cyfrowy. **Cyfrowy asystent**(*Digital assistant*) lub asystent wirtualny to program który może wykonywać zadania lub usługi na podstawie komend lub pytań otrzymanych od osoby jego wykorzystującej. Czasami termin „chatbot" również jest używany w odniesieniu do wirtualnych asystentów. «Chatbot» to asystent komunikacja z którym jest możliwa tylko przez komendy tekstowe, chat online, bez użycia komunikacji głosowej.

Zasady budowy i funkcjonowania Każdy asystent wirtualny składa się z trzech podstawowych elementów:

- Aplikacja lub strona internetowa za pomocą której klient będzie komunikować z asystentem.
- Moduł odpowiadający za przetwarzanie języka naturalnego (NLP model).
- Moduł który wykonuje otrzymaną komendę lub łączy asystenta z serwisami które w stanie przekazać odpowiedz na otrzymane pytanie od użytkownika.

Pierwszy element czyli aplikacja lub strona internetowa, najcześciej przedstawia sobą tylko interfejs dla zadania pytana lub wyświetlenia odpowiedzi i komunikacji z serwerem na którym umieszczone są inne elementy takiego systemu. Dodatkowo taka aplikacja może posiadać komendę podstawową dla aktywacji asystenta, na przykład «Ok Google» czy « Hej Siri». Taka komenda rozpoznawana jest lokalnie w bardzo uproszczonym modelu «Speech to text». Model jest uproszony przez to że pełne modeli rozpoznawania głosu i przetwarzania języka naturalnego wymagają nie malej mocy obliczeniowej często niedostępnej w urządzeniach na których asystent jest zainstalowany.

Drugiem elementem takiego systemu, jest moduł przetwarzania języka naturalnego, czyli moduł NLP. NLP to dziedzina, łącząca zagadnienia sztucznej inteligencji i językoznawstwa, zajmująca się automatyzacją analizy, rozumienia, tłumaczenia i generowania języka naturalnego przez komputer. Przetwarzanie języka naturalnego obejmuje wiele różnych technik interpretacji języka ludzkiego od metod statystycznych do uczenia maszynowego. Zadaniem NLP jest rozbicie języka na krótsze, elementarne kawałki i zrozumienie relacji między nimi.

Głównym zadaniem NLP w cyfrowych asystentach jest przetworzenie pytań lub komend użytkownika w postać oczyszczoną. Oczyszczanie tekstu składa się z 4 głównych elementów:

- **Tokenizacja**
- **Normalizacja**
- **Generalizowanie**
- **Usuwanie szumu**

Tokenizacja jest procesem, który dzieli tekst na tokeny (słowa lub zdania). Podział na tokeny pozwala na właściwe dalsze przetwarzanie słów („gwiazdozbiór" -> "zbiór gwiazd".

Normalizacja zapewnia spójność wyrazów poprzez sprowadzanie wszystkich liter do jednakowej wielkości, czy zamiany wszystkich słownie napisanych liczb na cyfry.

Proces generalizacji polega na sprowadzaniu słów do ich formy podstawowej (ujednoliceniu form wyrazów) za pomocą lematyzacji lub stemmingu. Lematyzacja to sprowadzanie formy fleksyjnej wyrazu do postaci słownikowej („w czerwcu" - > „w czerwiec"), natomiast stemming polega na usuwaniu przedrostków oraz przyrostków doprowadzając słowo do jego członu ('koty", „kocie" -> „kot").

Proces usuwania szumu ma za zadanie usuwanie części tekstu, która nie niesie informacji (interpunkcja, białe znaki, stop words / stop listy (słowa o małym znaczeniu (spójniki: „i", „oraz", „lub") oraz słowa popularne („mp3", „xd"), czasem też cyfry).

Moduł odpowiadający za przetwarzanie głosu w text w obecnie używanych asystentach może być zrealizowany na dwa sposoby:

- za pomocą **ukrytego modelu markowa** (HMM)
- za pomocą **głębokich sieci neuronowych.**

Proces Markowa – ciąg zdarzeń, w którym prawdopodobieństwo każdego zdarzenia zależy jedynie od wyniku poprzedniego.

HMM — proces Markowa, którego stany są ukryte, stany te odpowiadają fonemom mowy ludzkiej, połączenia między nimi mają wagi zależne od prawdopodobieństwa wystąpienia jednego fenomu po drugim. HMM dostaje rozkład prawdopodobieństw wystąpienia różnych fenomów w aktualnie badanym fragmencie dźwiękowym i następnie, na podstawie wiedzy jaki fenom wystąpił w poprzedniej analizie, uwydatnia wartości prawdopodobieństwa fenomów które na podstawie połączeń między jego stanami powinny wystąpić.

W pierwszym przypadku najpierw sygnał jest próbkowany a następnie odbywa się ekstrakcja cech. Sygnał jest dzielony na fragmenty i każdy fragment zostaje przekształcony na wektor cech. Dalej taki wektor podawany jest do modelu akustycznego. Ukryte stany HMM odpowiadają poszczególnym fonemom. Następnie słownik wymowy określa prawdopodobieństwo z jakim podana sekwencja fonemów składa się w wyraz a model językowy określa prawdopodobieństwo wystąpienia danej sekwencji słów w określonym języku.

Oczywiście niektóre elementy można zastąpić za pomocą głębokich sieci neuronowych, np realizacja ekstrakcji cech za pomocą DNN z ograniczoną liczbą wejść.

Aby uzyskać end to end ASR (automatic speech recognition) trzeba zamienić jak najwięcej części tradycyjnej HMM siecią neuronową.

Ostatni moduł najczęściej wyszukuje odpowiedz na pytanie w bazie wiedzy asystenta lub prosi zewnętrzne serwisy na udostępnię odpowiedzi na podane pytanie.

2.12.1 Zastosowania

Można wyróżnić kilka zastosowań asystentów cyfrowych:

- **Obywatelskie**
- **Wojskowe**
- **Medyczne**

Obywatelski:

- **Urządzenia mobilne**. W urządzeniach mobilnych asystenci cyfrowe najczęściej używane są dla wykonania prostych zapytań, np. kiedy ręce użytkownika są zajęte, informacja o pogodzie, lub o znanych faktach, ustawienie timera lub budzika, sprawdzenie zaplanowanych spotkań. Jeżeli wybrany asystent udostępnia API dla deweloperów może on również otrzymywać informacje od aplikacji które taki API wdrożyli, np. Informacja o ostatnim zamówieniu jedzenia

czy o ilości wykonanych kroków. Integracja z różnymi serwisami i urządzeniami umożliwia dodatkowe funkcjonalności asystentów np: włączenie muzyki na smart głośnikach, sterowania temperaturą w pomieszczeniu, włączenie i wyłączenie lampek. Niektóre asystenci pozwalają na komunikację z innymi osobami bez użycia głosu, np. Google Duplex. Duplex umożliwia rezerwacje usług w miejscach nie posiadających dostępnej rezerwacji online. Dodatkowo Duplex może odpowiadać na połączenie wchodzące gdy numer nie jest znany. Użytkownik w tym momencie widzi transkrypcje rozmowy i może rozpocząć samodzielnie odpowiadać w każdym momencie.

- **Inteligentne głośniki**. Inteligentne głośniki posiadają większość funkcjonalności dostępnych w urządzeniach mobilnych. Najczęściej one wykorzystywane gdy użytkownik nie ma dostępu do swojego telefonu lub jego użycie nie jest wygodne.
- **Samochody**. Istnieje trzy różnych podejścia do użycia asystentów cyfrowych w samochodach: Wykorzystanie asystenta wbudowanego w telefon (Android Auto lub Apple CarPlay) Zainstalowanie dodatkowego urządzenia z wbudowanym asystentem (Chris lub Mobileye) Całkowita integracja asystenta do systemów samochodu (Android Automotive OS, MBUX, BMW Intelligent Personal Assistant...)

  Android Auto lub Apple CarPlay za dość niski koszt pozwalają użytkownikowi połączyć swój telefon z ekranem multimedia swojego samochodu. Taka integracja pozwala użytkownikowi wykorzystywać wiele funkcji swojego telefonu, np nawigacja, włączenie muzyki na głośnikach, odpowiadać na połączenie wchodzące za pomocą mikrofonów i głośników samochodu. Jednak nie pozwala takie rozwiązanie na sterowanie samochodem.

  Zainstalowanie dodatkowego urządzenia pozwala wykonywać zaimplementowane przez producenta funkcji gdy samochód jest stary i nie posada możliwości integracji bezpośrednio z ekranem multimedia.

  Całkowita integracja asystenta do systemów samochodu pozwala na sterowania funkcjami samochodu, np włączenie ogrzewania krzesła, zmiana temperatury powietrza, otwarcie okna.

Wojsko:

- **Komunikacja z kandydatami** W niektórych krajach używany jest do interakcji z potencjalnymi żołnierzami aby poradzić im najlepszą profesje wojskową zgodnie z ich umiejętnościami.
- **Wspomaganie sterowaniem** W następnym pokoleniu okrętów wojennych będą zainstalowane asystenty głosowe aby ułatwić wykorzystanie niektórych funkcji, będzie dodatkowo ubezpieczony danymi biometrycznymi aby uniemożliwić użycie osób nieautoryzowanych.

  Rzadko używany na polu bitwy bo jest dojść łatwo imitować glos i uzyskać dostęp do informacji.

Medycyna:

- **Zastąpienie podstawowego personalu** Dobrym przykładem cyfrowego asystenta w medycynie jest chatbot zastępujący recepcjonistę w szpitalu. On nadaje takie same informacje jak i zwykła osoba jednak może w tym samym momencie pracować z dużą ilością osób. Jest używany w niektórych szpitalach Australii jako dodatkowy recepcjonista.
- **Terapia** Woebot to chatbot który jest używany dla terapii depresji. Nie zamienia on zwykłego lekarza a tylko dodatkowo pomaga pacjentowi.
- **Diagnozowanie chorób** Istnieją również Cyfrowi asystenci, które konsultują i udzielają po-

rady medyczne dla swoich użytkowników. Ich głównym celem jest pomoc pacjentom w znalezieniu rozwiązania dla najczęstszych symptomów. Zadaniem takich asystentów jest zapewnienie dostępnej i natychmiastowej pomocy tym, którzy nie mają szybkiego dostępu do zwyklej pomocy medycznej, jednak nie mogą oni jeszcze zastąpić lekarzy.