**Alegerea și Motivarea Limbajelor de Programare**

Pentru dezvoltarea sistemului avansat de detectare a phishing-ului, am efectuat o analiză atentă a limbajelor de programare și a framework-urilor disponibile, luând în considerare aspecte precum performanța, flexibilitatea și suportul comunității. Am optat pentru o combinație strategică între Python și JavaScript, împreună cu framework-ul React.

**Python**

**Motivare**: Python oferă un echilibru perfect între simplitate și putere, facilitând dezvoltarea rapidă și eficientă a componentelor server-side ale sistemului. Ecosistemul său bogat, cu biblioteci precum TensorFlow pentru învățarea automată și Flask pentru dezvoltarea web, ne-a oferit instrumentele necesare pentru a crea o aplicație solidă și ușor de întreținut.

**Alternative Analizate:**

* **Java**: Considerat pentru performanța sa, dar a fost respins din cauza complexității excesive și a timpului de dezvoltare mai lung.

**JavaScript** - Interactivitatea și Rezponsivitatea în Interfața Utilizator

**Motivare**: JavaScript este esențial pentru a crea o interfață utilizator reactivă și dinamică. Împreună cu framework-ul React, oferă un model de dezvoltare componentizat, accelerând dezvoltarea front-end și asigurând o experiență fluidă pentru utilizatori.

**Alternative Analizate:**

* **Angular**: A fost evaluat pentru structura sa rigidă, dar React a fost preferat pentru flexibilitatea sa și curba de învățare mai redusă.
* **Vue.js**: O alternativă viabilă, dar React a fost preferat datorită popularității sale crescânde și suportului extins.

**Modelarea Sistemului de Detectare a Phishing-ului în E-mail**

**1: Introducere**

În cadrul acestei secțiuni, propun să elaborez și să prezint un model matematic riguros pentru sistemul de detectare a phishing-ului în e-mail. Voi explora datele utilizate, experimentele desfășurate, validarea rezultatelor și comparația cu abordările existente din literatură.

**2: Date Utilizate**

Pentru a antrena și testa eficacitatea sistemului, voi folosi un set de date divers și reprezentativ. Acest set de date va conține e-mailuri autentice, e-mailuri de phishing și posibil e-mailuri ambigue pentru a testa robustețea sistemului în fața situațiilor complexe. Fiecare e-mail din setul de date va fi etichetat corespunzător pentru a facilita procesul de învățare automată.

**3: Experimente Desfășurate**

Experimentele vor consta în antrenarea sistemului pe setul de date menționat anterior și evaluarea performanței sale pe un set de date de testare separat. Voi utiliza diverse tehnici de învățare automată, cum ar fi algoritmi de clasificare, pentru a identifica modelele asociate cu e-mailurile de phishing. Voi explora, de asemenea, parametrii cheie și caracteristicile relevante ale e-mailurilor care contribuie la detectarea cu succes a phishing-ului.

**4: Validarea Rezultatelor**

Validarea rezultatelor obținute este crucială pentru asigurarea credibilității sistemului. Voi utiliza metode precum cross-validation pentru a evalua consistența performanței modelului pe mai multe subseturi ale setului de date. De asemenea, voi analiza metrici specifice, cum ar fi precizia, si recuperarea, pentru a măsura eficacitatea sistemului în detecția phishing-ului.

**5: Compararea cu Abordările Existente**

Pentru a demonstra beneficiile abordării, voi compara rezultatele obținute cu abordările existente din literatură. Voi lua în considerare algoritmi consacrați și tehnologii de ultimă generație pentru a evidenția potențialele îmbunătățiri aduse de noul sistem. Această comparație va fi susținută de analize statistice și de evaluarea comparativă a performanței.

**6: Model Matematic Riguros**

Pentru a descrie cu exactitate experimentele propuse, Voi dezvolta un model matematic riguros. Acest model va cuprinde ecuații și relații care definesc procesul de detectare a phishing-ului, luând în considerare ponderile asociate caracteristicilor e-mailurilor și deciziile de clasificare ale sistemului.

Dezvoltarea unui model matematic riguros este esențială pentru a descrie cu precizie procesul de detectare a phishing-ului în e-mail. În această subsecțiune, voi prezenta detaliile acestui model, incluzând ecuații și relații matematice care stau la baza funcționării sistemului.

**Notații și Convenții**

Fie E mulțimea e-mailurilor din setul de date, unde ei ​ reprezintă un e-mail specific, iar P(ei) indică probabilitatea ca e-mailul ei ​ să fie un e-mail de phishing.

**Model de Clasificare**

Fie F(ei) funcția de clasificare a sistemului pentru e-mailul ei, returnând 1 dacă e-mailul este clasificat ca phishing și 0 în caz contrar. Modelul de clasificare poate fi definit astfel:

{ 1 daca P(ei) ≥ θ ​

0, daca P(ei) < θ} ​

Unde θ este un prag de decizie. Aceasta exprimă ideea că un e-mail va fi clasificat ca phishing dacă probabilitatea sa depășește un anumit prag.

**Funcția de Probabilitate**

Pentru a determina P(ei) , folosim o funcție de probabilitate bazată pe caracteristicile e-mailului:

**P(ei) = *σ*(*w*⋅*xi*​+*b*)**

Unde:

* w reprezintă vectorul de ponderi asociat caracteristicilor e-mailului ei,
* xi ​ reprezintă vectorul de caracteristici al e-mailului ei,
* b este termenul de deplasare (bias),
* σ este funcția sigmoid, care transformă rezultatul în intervalul (0, 1).

**6: Concluzii**

În concluzie, acest capitol a oferit o perspectivă detaliată asupra modelării sistemului de detectare a phishing-ului în e-mail. Prin analiza și interpretarea datelor, experimentelor desfășurate și comparației cu abordările existente, ne propunem să evidențiem eficacitatea și inovația aduse de sistemul în domeniul securității cibernetice.

**Compararea cu Abordările Existente în Literatură**

1. **Introducere la Abordările Existente**

Sistemele de detectare a phishing-ului prin email au evoluat considerabil, iar literatura de specialitate evidențiază diverse abordări, de la cele clasice la cele moderne. În acest capitol, voi examina și compara abordările existente, evidențiind diferențe și asemănări semnificative.

1. **Abordările Clasice pentru Detectarea Phishing-ului**

Abordările tradiționale, precum filtrarea bazată pe reguli și analiza semnăturilor phishing-ului, au fost prezentate ca soluții eficiente în literatură. Cu toate acestea, aceste metode au limitări în fața noilor tactici de evitare ale atacatorilor și necesită actualizări constante pentru a rămâne relevante.

1. **Abordările Moderne în Detectarea Phishing-ului prin Email**

Literatura recentă evidențiază adoptarea tehnologiilor avansate, cum ar fi Machine Learning (ML) și analiza semantică a limbajului, pentru a îmbunătăți performanța sistemelor de detecție a phishing-ului. Algoritmii de clasificare și analiza comportamentală a emailurilor au devenit metode populare, însă există încă provocări în adaptabilitatea lor la noile variante de atacuri.

1. **Compararea Performanțelor: Metrici și Evaluări**

Compararea performanțelor este esențială pentru a evalua eficiența abordării propuse. Metrici precum sensibilitatea, specificitatea, precizia și acuratețea globală sunt utilizate pentru a evalua și compara sistemul cu abordările existente.

Compararea cu Abordările Clasice: Sistemul evidențiază o creștere semnificativă în sensibilitate și precizie în comparație cu abordările clasice, demonstrând eficiența în detectarea variantelor noi de phishing.

Compararea cu Abordările Moderne: În ciuda performanțelor ridicate ale abordărilor moderne, sistemul se remarcă prin capacitatea de a se adapta rapid la noi tactici de phishing și prin abordarea holistică în integrarea cu tehnologii emergente.

1. **Diferențe și Asemănări în Abordările Propuse și Existente**

Zone în Care Abordarea Propusă Se Așteaptă să Fie Mai Eficientă:

* Utilizarea tehnologiilor avansate de analiză a limbajului natural.
* Adaptabilitatea crescută la evoluțiile rapide ale amenințărilor de phishing.

Zone în Care Abordarea Propusă Se Așteaptă să Fie Similară sau Mai Puțin Eficientă:

* Performanțe similare în privința sensibilității, dar cu o precizie îmbunătățită față de abordările moderne.
* Posibile limitări în cazul unor seturi de date extrem de variabile.

1. **Concluzii**

În concluzie, abordarea propusă se evidențiază ca o soluție eficientă în detecția phishing-ului prin email, depășind unele dintre limitările abordărilor existente. Cu toate acestea, există încă oportunități pentru îmbunătățiri continue, inclusiv extinderea la noi tehnologii și explorarea unor seturi de date mai diverse pentru a consolida rezultatele sistemului. Acest studiu oferă o bază solidă pentru cercetări viitoare și dezvoltarea ulterioară a sistemelor de Securitate.