**پروژه: طراحی و پیاده‌سازی چارچوب رمزنگاری کوانتومی-مقاوم هیبریدی با استفاده از شبکه‌های عصبی و رمزنگاری همومورفیک**

**نام پروژه:** **NeuroQuanticrypt**

1. **هدف اصلی پروژه (The "Big Idea")**

ایجاد یک چارچوب رمزنگاری که:

1. **مقاوم در برابر کامپیوترهای کوانتومی** باشد (Post-Quantum Cryptography).
2. از **یادگیری ماشین** برای ایجاد مدل‌های رمزنگاری پویا و مبتنی بر الگوی داده‌ها استفاده کند.
3. قابلیت **محاسبه روی داده‌های رمز شده** (Fully Homomorphic Encryption - FHE) را برای کاربردهای ابری فراهم کند.
4. از یک **مدل اعتماد صفر (Zero-Trust)** پیروی کند، به طوری که حتی ارائه‌دهنده سرویس نیز نتواند به داده‌های خام دسترسی داشته باشد.

این پروژه سه لایه امنیتی مستقل اما یکپارچه ایجاد می‌کند.

1. **اجزای اصلی**

**الف) لایه اول: رمزنگاری مبتنی بر شبکه عصبی (Neural-Based Dynamic Encryption - NDE)**

* **نوآوری:** به جای استفاده از توابع ثابت ریاضی مانند AES یا RSA، از یک شبکه عصبی برای تولید جریان کلید (Keystream) استفاده می‌شود. این شبکه بر اساس خود داده‌ی ورودی (Plaintext) و یک کلید اصلی (Master Key)، یک الگوی رمزنگاری منحصربه‌فرد تولید می‌کند.
* **مکانیزم:**
  1. **آماده‌سازی:** داده به بلوک‌های n-بایتی تقسیم می‌شود.
  2. **تولید جریان کلید:** یک شبکه عصبی سبک‌وزن مانند یک شبکه کانولوشنی کوچک یا LSTM هر بلوک را دریافت کرده و یک دنباله بایت تصادفی پیچیده (Keystream) تولید می‌کند. وزن‌های این شبکه با استفاده از کلید اصلی و یک Salt مقداردهی اولیه می‌شوند.
  3. **رمزنگاری:** یک عملگر XOR ساده بین بلوک داده و جریان کلید تولیدشده انجام می‌شود.
  4. **پویایی (Dynamic):** پس از رمز کردن هر بلوک، خروجی شبکه عصبی بر اساس یک تابع بازخورد، به ورودی بلوک بعدی تزریق می‌شود. این کار الگوی رمزنگاری را برای هر بلوک وابسته به بلوک قبلی می‌کند و در برابر تحلیل الگو بسیار مقاوم است.

**ب) لایه دوم: رمزنگاری کوانتومی-مقاوم (Post-Quantum Layer - PQL)**

* **نوآوری:** استفاده از یک الگوریتم استاندارد و مورد تایید **CRYSTALS-Kyber** برای تبادل کلید یا  برای امضا به عنوان یک لایه مستقل اما یکپارچه.
* **مکانیزم:**
  1. کلید اصلی (Master Key) مورد استفاده در لایه NDE، خود با الگوریتم Kyber رمزگذاری می‌شود.
  2. این کلید رمز شده سپس در هدر فایل رمزگذاری شده ذخیره می‌گردد.
  3. برای رمزگشایی، ابتدا باید کلید اصلی با استفاده از کلید خصوصی Kyber بازیابی شود. این کار امنیت سیستم را حتی در صورت شکست لایه عصبی نیز تضمین می‌کند.

**ج) لایه سوم: رمزنگاری همومورفیک انتخابی (Selective Homomorphic Encryption - SHE)**

* **نوآوری:** این لایه امکان انجام محاسبات خاص (مانند جمع یا ضرب) را روی داده‌های رمز شده لایه NDE فراهم می‌کند، بدون نیاز به رمزگشایی کامل.
* **مکانیزم:**
  1. از یک طرح رمزنگاری همومورفیک سبک‌وزن استفاده می‌شود.
  2. این لایه به صورت اختیاری و فقط برای فیلدهای دادهای خاص که نیاز به پردازش ابری دارند (مثلاً "سن" یا "مبلغ تراکنش") فعال می‌شود.
  3. داده‌های مربوط به این فیلدها یک بار دیگر با FHE رمز می‌شوند و به همراه داده‌های رمز شده اصلی ذخیره می‌گردند.

**3. نمودار گردش کار (Workflow)**

****

* 1. **مزایای کلیدی و نوآوری‌ها**

1. **امنیت سه لایه:** شکستن یک لایه به معنای دستیابی به داده‌ها نیست.
2. **مقاومت در برابر کوانتوم:** هسته اصلی سیستم بر پایه رمزنگاری کوانتومی-مقاوم است.
3. **پویایی و تطبیق‌پذیری:** لایه عصبی (NDE) الگوی رمزنگاری را بر اساس داده‌ها تغییر می‌دهد، که تحلیل رمز را بسیار سخت می‌کند.
4. **قابلیت پردازش ابری امن:** لایه FHE امکان استفاده از قدرت پردازشی ابر بدون به خطر افتادن حریم خصوصی را فراهم می‌کند.
5. **مدل اعتماد صفر:** کلید اصلی فقط نزد کاربر نهایی است. داده‌های موجود در ابر به طور کامل رمز شده و غیرقابل خواندن هستند.
   1. **چالش‌های فنی و حوزه‌های تحقیق**

* **بهینه‌سازی عملکرد:** شبکه‌های عصبی و FHE بسیار سنگین هستند. نیاز به تحقیق بر روی معماری‌های بهینه و سخت‌افزارهای خاص (مانند GPU/TPU) دارید.
* **امنیت لایه عصبی:** باید ثابت شود که شبکه عصبی به اندازه الگوریتم‌های استاندارد امن است. تحلیل امنیتی این بخش بسیار پیچیده است.
* **مدیریت کلید:** طراحی یک سیستم مدیریت کلید امن و مقیاس‌پذیر برای کلید اصلی و کلیدهای Kyber.
* **استانداردسازی:** این یک طرح جدید است و نیاز به بررسی‌های گسترده توسط جامعه رمزنگاری دارد.
  1. **کاربردهای بالقوه**
* **امنیت داده در رایانش ابری:** برای شرکت‌هایی که داده‌های حساس را در ابر ذخیره می‌کنند اما نیاز به انجام Query و تحلیل روی آن‌ها دارند.
* **حفاظت از داده‌های پزشکی (Health Data):** امکان اشتراک‌گذاری داده‌های بیماران بین مراکز تحقیقاتی بدون افشای اطلاعات شخصی.
* **امنیت در سیستم‌های مالی و بانکی:** برای محافظت از تراکنش‌ها و اطلاعات مشتریان در برابر تهدیدات آینده (کوانتومی).
* **سیستم‌های نظامی و دولتی:** برای محرمانه نگه داشتن اطلاعات در بالاترین سطح.