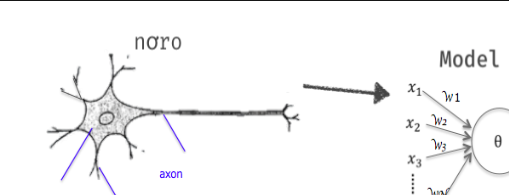
**Survey về tấn công dữ liệu nhạy cảm trong machine learning**

**Khảo sát về dữ liệu nhạy cảm trong machine learning**

* Dữ liệu nhạy cảm là dữ liệu có thông tin mật , thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng , tài chính hoặc hoạt đông của đơn vị , cá nhân hoặc một doang nghiệp nào đó.

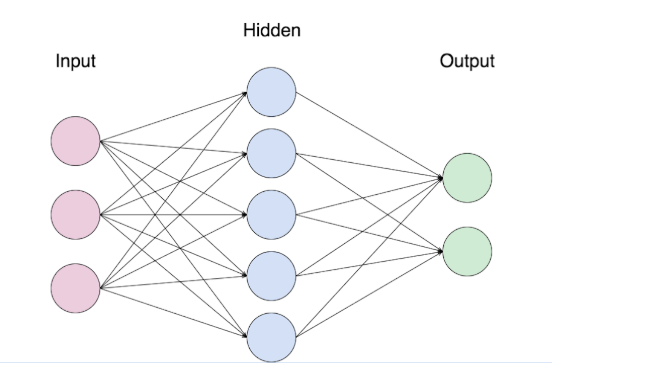
1. **Tổng quan về Deep Learning & Neural Network**
2. **Neural & Neural Network**

* **Neural** là mô hình toán học mô phỏng và biểu hiện cho một số chức năng của nơron thần kinh trong não bộ con người (Xem hình bên dưới)

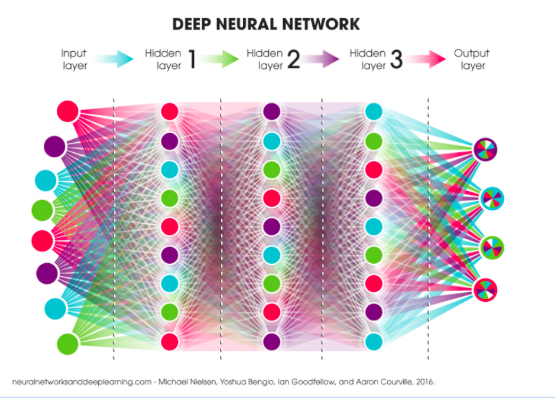


**Neural là mô hình toán học mô phỏng nơron thần kinh con người.**

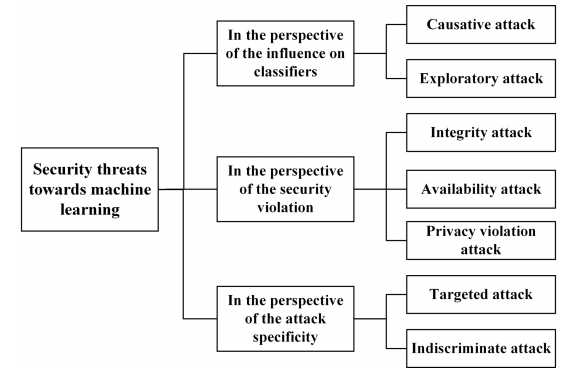
* **Neural Network:** là tập hợp của nhiều Neural, các tập hợp này tạo thành một cấu trúc hệ thống gồm các lớp mà ta còn gọi là các layer. Trong đó, ta sẽ thấy một Neural Network đơn (Simple Neural Network) hay một đơn vị Neural Network thường có các lớp: Input layer (lớp đầu vào), Hidden layer (lớp ẩn) và Output layer (lớp đầu ra).



Sơ đồ mô phỏng cấu trúc một neural network đơn



Ta có thể hình dung cấu trúc của Deep Neural Network như hình trên.



Hình ảnh phân loại các mối de dọa trong machine learning