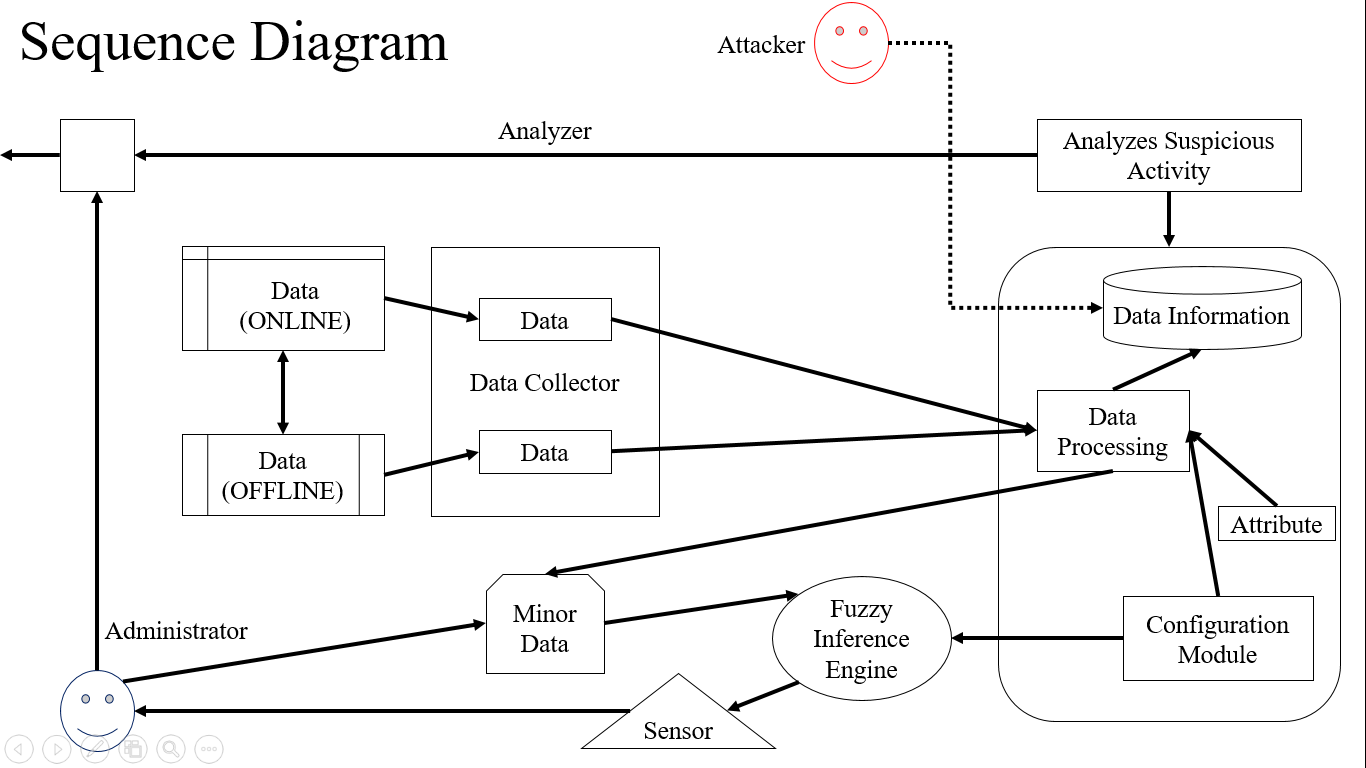
In this diagram, we can see the data is online and offline, and an attacker will try to access to the information and the sensor inform to the administrator to update and change the information and send further.



AI in Intrusion Detection System

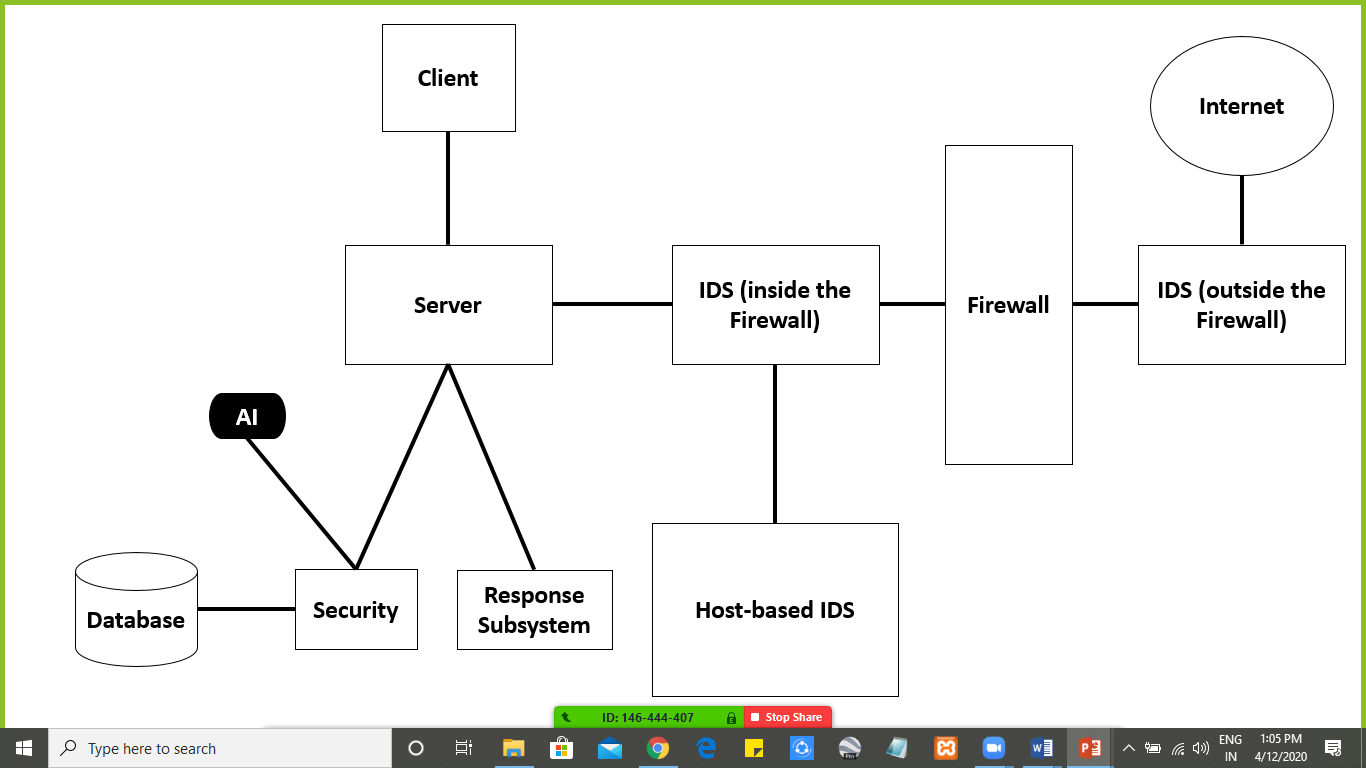
“In IDS, using AI for security would help us to recognize the **user** so that an intruder couldn’t access to the security breach and our database information is secured.”

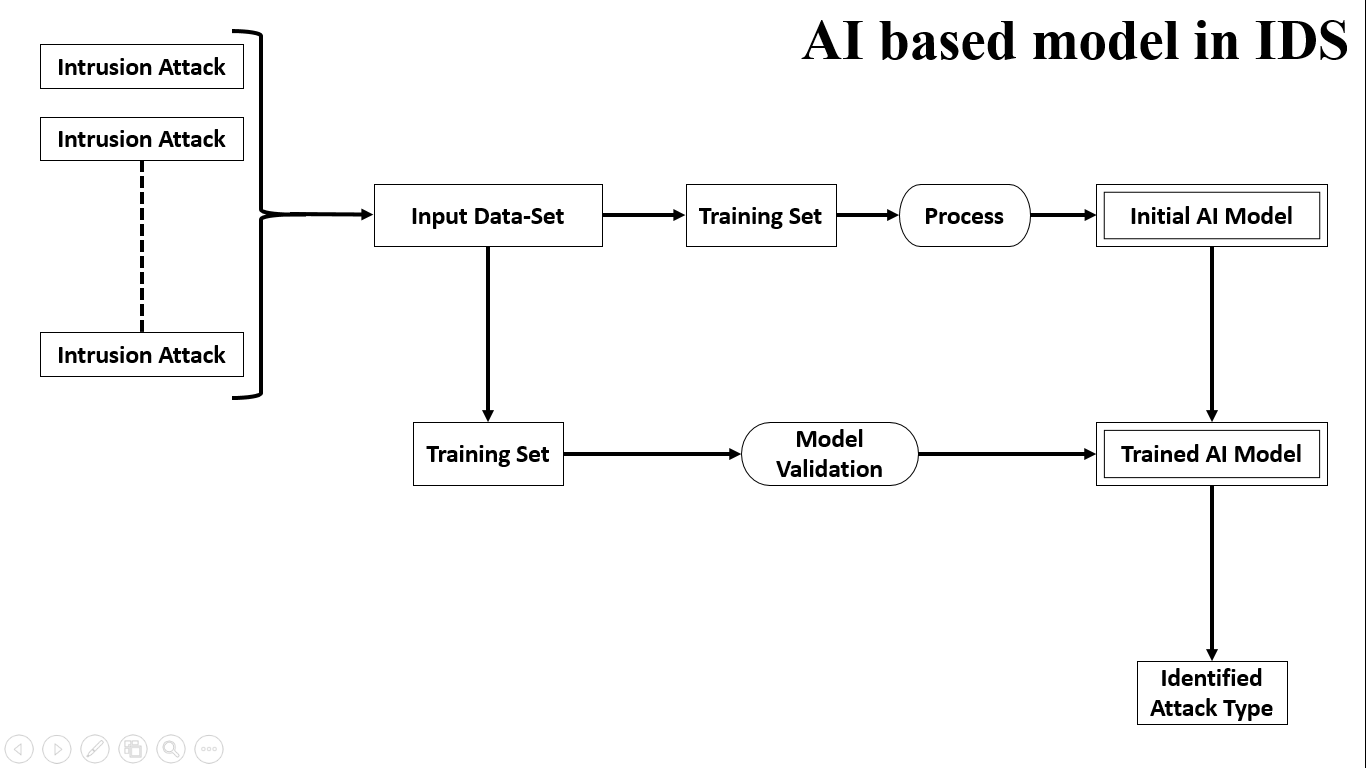
**IDS implementation using AI**

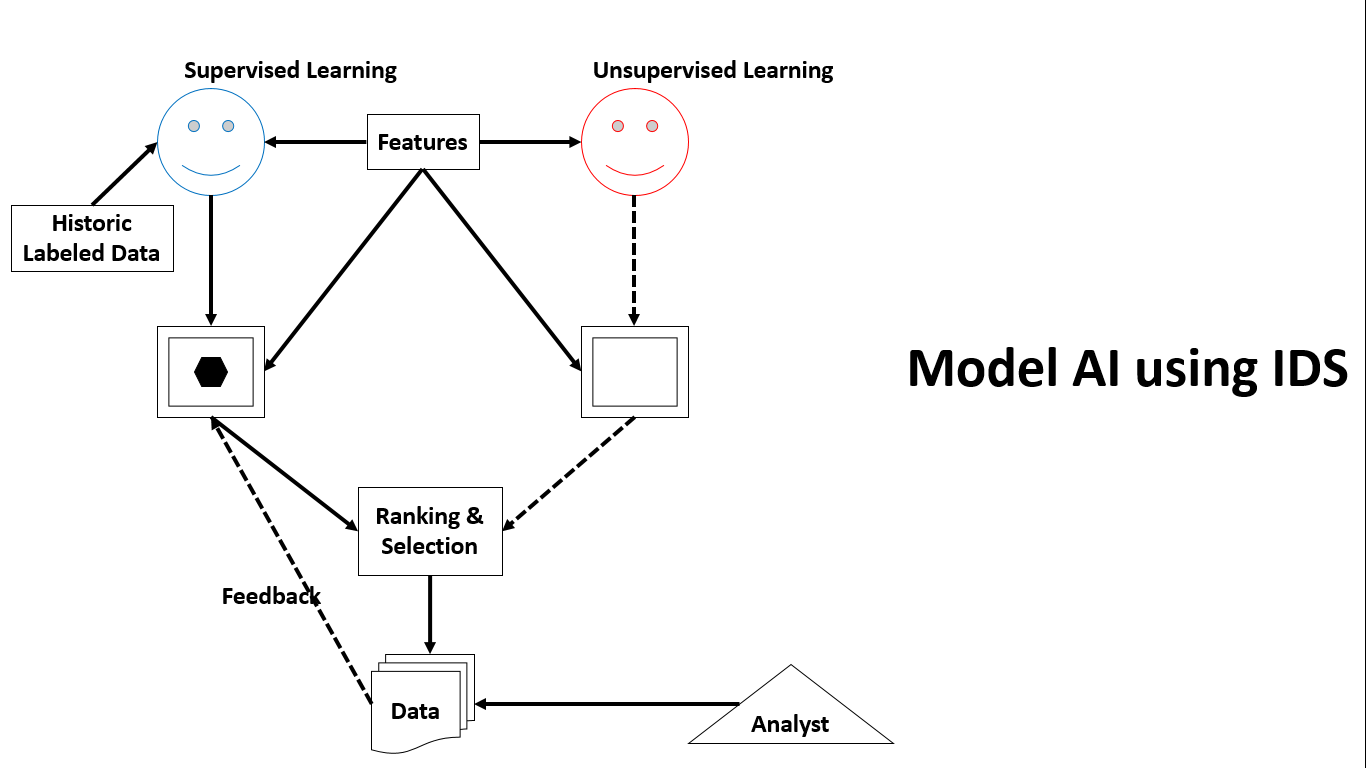
Artificial intelligence has been widely used in decision-making system and for the classification in [computer vision](http://www.scialert.net/asci/result.php?searchin=Keywords&cat=&ascicat=ALL&Submit=Search&keyword=computer+vision) applications. It is utilized in various [processing](http://www.scialert.net/asci/result.php?searchin=Keywords&cat=&ascicat=ALL&Submit=Search&keyword=image+processing) applications including [face, finger or voice recognition](http://scialert.net/asci/result.php?searchin=Keywords&cat=&ascicat=ALL&Submit=Search&keyword=pattern+recognition).

AI can be classified in supervised, unsupervised and hybrid learning methods.

In supervised learning, desired output is used to learn the algorithm for better classification, whereas in unsupervised AI inputs are analyzed without target output. Hybrid approach integrates both supervise and unsupervised learning method to generates specified rules and or signature. The block diagram for AI based intrusion detection system.







IDPS components, including sensors, event databases, and management consoles must integrate with a network-wide monitoring capability.

