LLM (Large Language Models)

A Breakdown from Eclypses CIO, Jefferson Dance

Large Language Models

LLM (Large Language Models) agents are an over-arching moniker for systems that analyze data and come to guided conclusions using Artificial Intelligence engines. Chat-GPT is a very popular one that is in wide use today. They are quite complex (and frankly - I do not pretend to understand all of their internal complexities). If you really want to dive into the guts, you can look at this article from NVIDIA (they have a vested interest due to the GPU's that they market and are widely used in Al engines).

Source: https://developer.nvidia.com/blog/introduction-to-llm-agents/

However, the collection of that data relies on either intentional feeding, the ability to scrape information from public sources, or in-transit data flows. If a web page shows information publicly, a bad-actor can scrape that information (read it off the glass) and then input that into their LLM. There are no safeguards against that since the data is shown in a human readable format.

Using Eclypses MTE Technology

When an application utilizes Eclypses MTE technology, and a bad-actor intercepts that message in mid-flight (man-in-the middle), it is completely useless as an input to an LLM. The key take-away here is that along with the secure coding practices, Eclypses MTE increases data security and adds a another layer of security on top of that.

In the event a bad-actor gains access to an API which serves up the data for the web/mobile app, and then attempts to access it using stolen credentials, if that API and its front-end app use Eclypses MTE technology,

the bad-actor is shut down at the front door! Only paired partners can access and retrieve data from a partner/protected API. Eclypses MTE allows AI organizations and developers the advantage of maintaining data integrity, security and access while ensuring clean, pure data for the business to utilize.

If a BOT attempts a brute-force attack on an API protected by Eclypses MTE, hoping to gain access to credentials, the API will never answer the BOT since the incoming credential request will be protected by a paired Eclypses MTE client. This will ensure that the API will not be able to decode the request to answer it.

Interestingly, the referenced article indicates that if a system is using "best practices" the bad-actor's LLM Agent has a low success rate. Unfortunately, this may lull an organization into a sense of complacency, which can be very dangerous.

With the secure MTE Relay, the effort to protect existing (and potentially vulnerable) web and mobile applications is minimal; especially now with automated deployment via cloud marketplaces). When an enterprise hosts their backend API on AWS, Eclypses MTE is a complete data security solution that protects data from Web, to Mobile, and to API and can be set as a policy to protect third party access and data sharing.



Doc ID: Eclypses-1532395320-501 Version: 3.0

Leveraging Eclypses MTE for LLM and Al

Eclypses MTE is poised to become the leader is data security around LLM and AI applications. The unique properties around Eclypses MTE enable AI platforms to leverage Eclypses MTE to solve these major challenges:

Establish and secure all data (PII, confidential and credentials) from ingestion through to consumption across all major access points and WEB, MOBILE, and API 3

clean, Pure DATA, without the ability to scrape, inject, grab credentials, or otherwise tamper with the data stream. Eclypses MTE offers a significant competitive advantage to Al firms in keeping their secure, providing data integrity and clean, pure and uncontaminated, data.

4

Leap Frog Compliance

Eclypses MTE represents the quickest and easiest way to upgrade and enhance your data security posture, while reducing risk and the material impact of a breach.

2

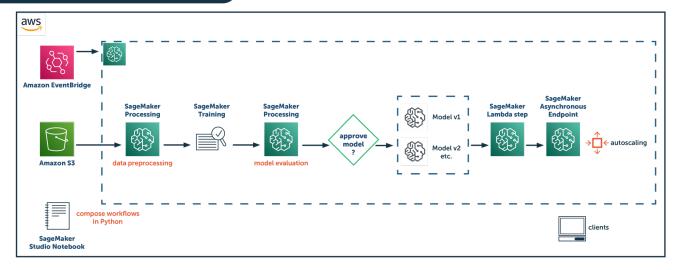
Enable AI and LLM to set Eclypses MTE as a policy for both consumption and third-party sharing, thereby ensuring that no data is at risk of being breached without direct access to the data base itself.

5

Network and Data security in one product, no need for VPNs or Web Application firewalls great for OP/EX enhancement. Secure logon from any network anywhere, globally. Eclypses MTE will not respond to any requests not encoded properly with Eclypses MTE.

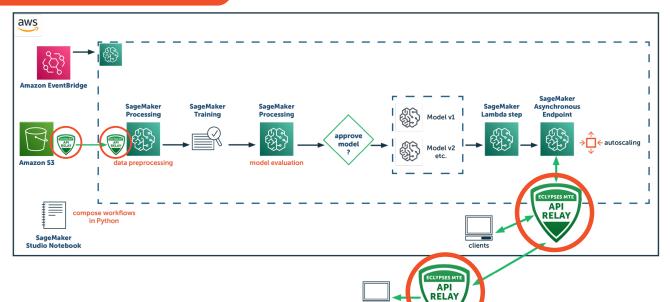
Eclypses MTE for AWS | Al Model Pipeline

AI Model without Eclypses MTE



Data in transit is left vulnerable if not safeguarded by Eclypses MTE.

Al Model with Eclypses MTE



With Eclypses MTE in place, data in transit is fully secured and protected from potential threats.