AI POWERED SPAM CLASSIFIER

TEAM MEMBERS :

1. SHAM SURESH S	(au951221104050)
2. M.E.ARUN MARIAPPAN	(au951221104006)
3. R.SIVAKAVIYARAGAVAN	(au951221104052)
4. A.A.MOHAMED ARSATH	(autjpcoelecs01)
5. R.SANJAY	(au951221104041)

PHASE II : INNOVATIONS

The root cause of spam emails can be attributed to several factors, but they primarily stem from the ease of sending bulk messages over the internet and the potential financial gains for spammers. Here are some key factors contributing to the proliferation of spam:

1. **Low Cost and High Returns:** Sending emails is incredibly cheap, and even if a tiny fraction of recipients respond to a spam message, spammers can still make a profit.

2. **Anonymity:** The internet allows for a degree of anonymity, making it difficult to trace the source of spam emails back to the sender. This anonymity emboldens spammers to send unsolicited messages without fear of direct consequences.

3. **Email Harvesting:** Spammers use various methods to harvest email addresses, such as web scraping, purchasing email lists, or using malware to collect addresses from infected computers.

4. **Phishing and Scams:** Many spam emails are designed to trick recipients into revealing personal information, such as passwords or credit card numbers, through phishing attacks. These emails often appear legitimate, making it more likely for recipients to fall victim to scams.

5. **Unsolicited Commercial Emails (UCE):** Some spam emails are simply advertisements for products or services. These messages are sent in bulk to a wide audience, hoping that a small percentage of recipients will make a purchase.

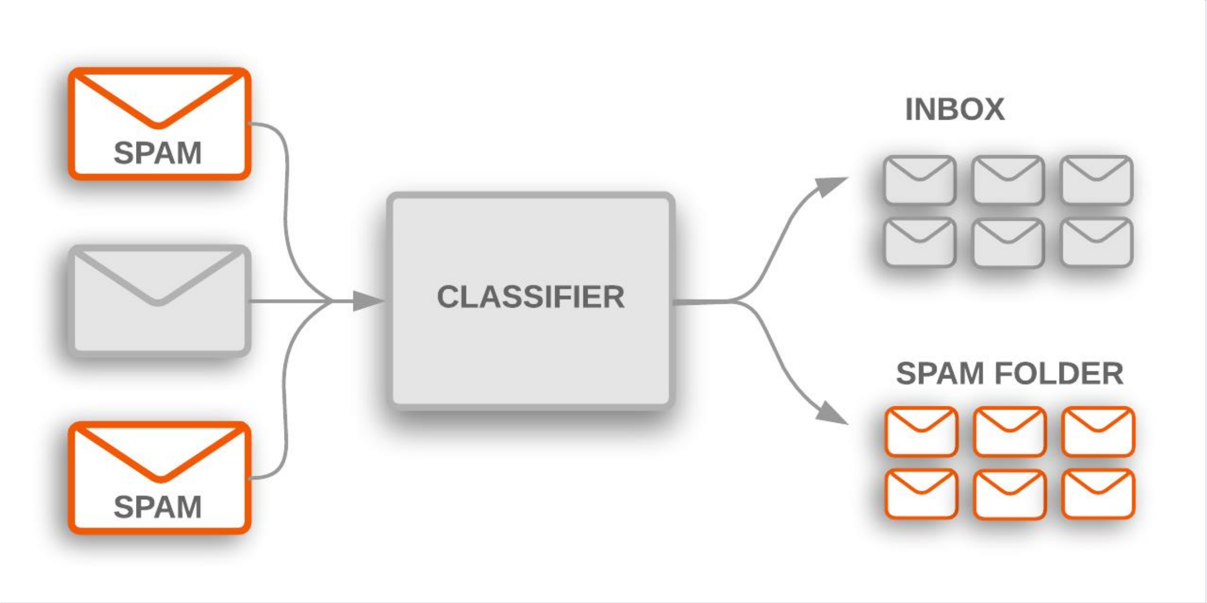
6. **Botnets and Malware:** Spammers often use botnets, networks of compromised computers controlled remotely, to send massive volumes of spam. Malware-infected computers can be turned into zombies, unknowingly sending out spam emails without the user's knowledge.

7. **Lack of Regulation:** The internet spans across different jurisdictions, making it challenging to enforce uniform anti-spam laws globally. Varying regulations and enforcement capabilities contribute to the persistence of spam.

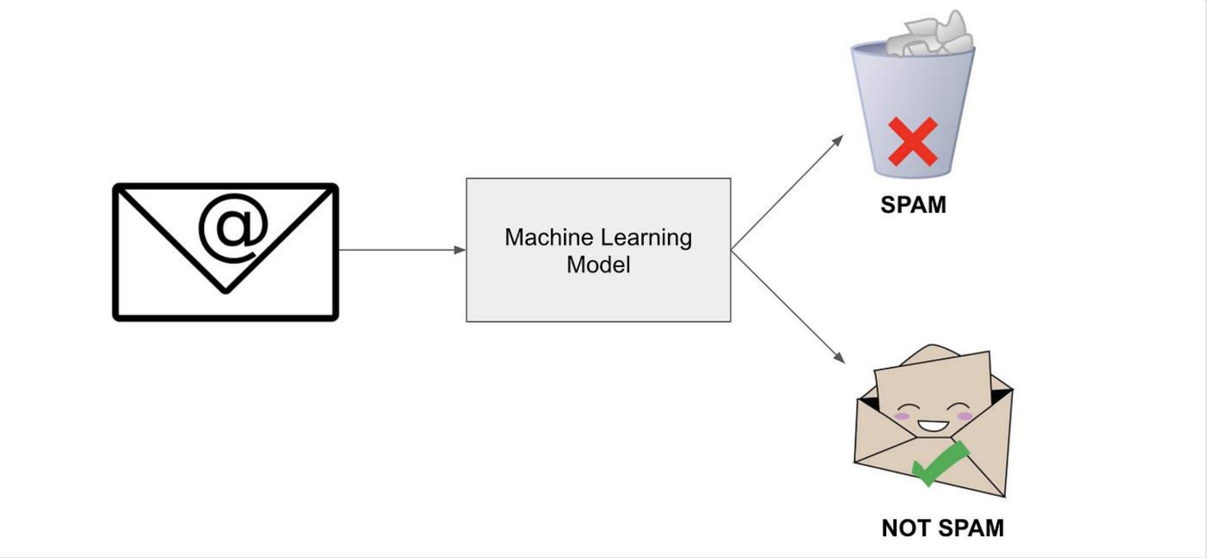
8. **Email Spoofing:** Spammers can forge the sender's address to make it appear as if the email is coming from a trusted source. This technique makes it difficult for recipients to distinguish between genuine and spam emails.

9. **Inadequate Security Measures:** Some email servers and clients might have vulnerabilities that spammers exploit to send spam messages. Inadequate security measures, such as weak passwords or outdated software, can facilitate unauthorized access to email accounts.

BLOCK DIAGRAM :



SAMPLE MODEL :



CONCLUSION :

From using there models such as associated with the AI and machine learning concepts we can create a AI based spam classifier which can be used to separate spams and ham from a set of online or transactional data.